Google Inc. et al v. Egger et al
Doc. 475 Att. 1

Exhibit 1

Dockets.Justia.com

TRANSCRIPT

May 15, 2007

COMMITTEE HEARING

SEN. PATRICK J. LEAHY
CHAIRMAN

SENATE JUDICIARY COMMITTEE
WASHINGTON, D.C.

SEN. PATRICK J. LEAHY HOLDS A HEARING ON THE U.S. ATTORNEY FIRINGS

CQ Transcriptions, LLC
1255 22nd Street N.W.
Washington, D.C. 20037
Transcript/Programming: Tel. 301-731-1728
Sales: Tel. 202-419-8500 ext 599
sales@cq.com
www.cq.com

Copyright 2007 CQ Transcriptions, LLC
All materials herein are protected by United States copyright law and may not be reproduced, distributed, transmitted, displayed, published or broadcast without the prior written permission of CQ Transcriptions. You may not alter or remove any trademark, copyright or other notice from copies of the content.

U.S. SENATE JUDICIARY COMMITTEE HOLDS A HEARING ON THE U.S. ATTORNEY FIRINGS

MAY 15, 2007

SPEAKERS:

SEN. PATRICK J. LEAHY, D-VT.
CHAIRMAN

SEN. EDWARD M. KENNEDY, D-MASS.

SEN. JOSEPH R. BIDEN JR., D-DEL.

SEN. HERB KOHL, D-WIS.

SEN. DIANNE FEINSTEIN, D-CALIF.

SEN. RUSS FEINGOLD, D-WIS.

SEN. CHARLES E. SCHUMER, D-N.Y.

SEN. RICHARD J. DURBIN, D-ILL.

SEN. SHELDON WHITEHOUSE, D-R.I.

SEN. BENJAMIN L. CARDIN, D-MD.

SEN. ARLEN SPECTER, R-PA.

RANKING MEMBER

SEN. ORRIN G. HATCH, R-UTAH

SEN. CHARLES E. GRASSLEY, R-IOWA

SEN. JON KYL, R-ARIZ.

SEN. JEFF SESSIONS, R-ALA.

SEN. LINDSEY GRAHAM, R-S.C.

SEN. JOHN CORNYN, R-TEXAS

SEN. SAM BROWNBACK, R-KAN.

SEN. TOM COBURN, R-OKLA.

WITNESSES:

FORMER DEPUTY ATTORNEY GENERAL JAMES B. COMEY

SCHUMER: I have a brief opening statement. I'm sure Senator Specter does. And then we'll get right into the questions.

First, I want to thank and commend Chairman Leahy for his continued leadership on the critically important issue of the politicization of the Justice Department. This is our committee's fifth hearing in four months focusing on the mass firing of almost 10 percent of our country's top federal prosecutors.

At our last hearing, on April 19th, Attorney General Gonzales attempted to justify the dismissals, explain his role, and put the matter behind him. He failed miserably in that attempt.

Indeed, four weeks later, the dismissals remain unexplained, the attorney general's role is murkier than ever, and with each new revelation, retraction and resignation the issue remains planted on the front pages, hobbling the department's ability to get its important work done.

Let me briefly review some of the developments since the attorney general's ill-fated appearance before this committee on April 19th.

Since April 19th, the former deputy attorney general, who is here today, has contradicted other DOJ officials by testifying that most of the fired U.S. attorneys performed well. We will be hearing more about that today.

Since April 19th, former Missouri U.S. attorney Todd Graves has come forward to say that he was also asked to resign in 2006. That brings the number of dismissals to at least nine and counting, not the eight that Mr. Gonzales testified to.

We'll be hearing more about that situation when the committee considers authorizing Chairman Leahy to subpoena Mr. Graves and his replacement, Bradley Schlozman.

Since April 19th, we've learned that a political corruption case involving Republicans in Arizona may have been slow-walked until after the 2006 election, as the Wall Street Journal has reported.

U.S. Attorney Paul Charlton's unhappiness with the pace of approvals from Washington may have led to his ouster. We'll be hearing more about that if and when the department responds to our request for information and documents.

And since April 19th, we have learned that one of the attorney general's top advisers, Monica Goodling, may have been doing the unthinkable: imposing a political and ideological litmus test in the hiring of career-level prosecutors and department lawyers.

We'll be hearing more about that when Ms. Goodling soon testifies under a grant of immunity.

And, of course, just yesterday, we learned of the latest and most high-ranking casualty of the current imbroglio. Mr. Comey's successor to the number two position at the department, Paul McNulty, announced his resignation.

The attorney general could almost wallpaper his office with the resignation letters of those who he was supposed to be supervising.

SCHUMER: The majority of people in his top circle are now no longer at the Justice Department.

Kyle Sampson, who was responsible for putting together the final firing list, has resigned. Monica Goodling, who helped with the list and served as the department's liaison to the White House, has resigned. Mike Battle, who was ordered to fire seven U.S. attorneys last December 7th, has resigned. And, of course, now the deputy attorney general himself has decided to resign.

I heard today that Attorney General Gonzales was trying to assign blame to Paul McNulty for the firings of the U.S. attorneys, saying that he relied on McNulty's advice. That's ironic, because Paul McNulty came clean with this committee and gave us some valuable information while the attorney general stonewalled.

The attorney general is trying to make Mr. McNulty into the next Scooter Libby, but we all know the buck stops with the attorney general.

Mr. Gonzales said at this hearing -- at that these -- Mr. Gonzales said in this hearing room that he accepts responsibility for the firings. Well, he should live up to his words and not keep pointing the finger today at Mr. McNulty.

There's been a -- there's long been reason to be concerned about Attorney General Gonzales given his close connection with the White House and his apparent misconception of this current role. He seems to many in this country to embody a disrespect for the rule of law and intolerance of independence at the Justice Department.

He's presided over a Justice Department where being a, quote, "loyal Bushie" seems to be more important than being a seasoned professional, where what the White House wants is more important than what the law requires or what prudence dictates.

The current scandal merely crystallizes this problem, namely that loyalty to the White House trumps allegiance to the law, the truth and common sense.

For example, Attorney General Gonzales' former chief of staff has testified that one of the principal reasons the A.G. was upset after listening to Mr. McNulty's testimony on February 6th was that Mr. McNulty had talked too much about the White House's role in appointing Karl Rove's deputy as U.S. attorney in Arkansas.

SCHUMER: Specifically, Mr. Sampson said Gonzales was upset that McNulty had, quote, "put so much emphasis on the White House's role in Griffin being promoted in favor of Cummins," unquote. Gonzales was upset because Mr. McNulty, quote -- said, quote -- Gonzales was upset because Mr. McNulty, quote, "had really brought the White House's role in Griffin into the public sphere."

So it appears that the attorney general was apparently not upset that Mr. McNulty had overstated the White House's role or misstated that role. He was only upset that he had exposed it. And now it appears that Mr. McNulty is gone because of it.

We've only begun to understand the White House's role in the firings and the attorney general's role in accomplishing the White House's bidding. So far, however, we know this at least.

It was the White House that initially raised the prospect of firing all 93 U.S. attorneys.

It was the White House that promoted the idea of removing Bud Cummins in favor of a former aide to Karl Rove.

It was the White House that was upset at the department's belated rejection of a plan to bypass homestate senators in Arkansas to keep Tim Griffin installed indefinitely as U.S. attorney.

It was the White House that had the best opportunity to correct the record of its own involvement in the firing at a March 5th meeting attended by Karl Rove before Mr. Moschella gave incomplete testimony to Congress.

It was the White House that entertained complaints from Republican Party officials about David Iglesias which apparently led to his ouster.

It was the White House that had brought overblown complaints about voter fraud prosecutions to the attention of the Justice Department.

There'll be time for us to hear from those White House witnesses who can shed light on what transpired here, and I hope the day comes soon.

Senator Specter?

SPECTER: Thank you, Mr. Chairman.

I join in the welcome of you, Mr. Comey.

SPECTER: It is ironic in a sense that the former deputy attorney general should be with the Judiciary Committee today, on the same day that we learn of the resignation of the present deputy attorney general.

Earlier today, I wrote to Deputy Attorney General Paul McNulty congratulating him on his service with the Department of Justice, and wishing him well in his new career.

I did not say in the note to him what I'm about to say, but I think he found it difficult -- really, impossible -- to continue to serve in the Department of Justice as a professional, which Paul McNulty is, because it's embarrassing for a professional to work for the Department of Justice today.

We had the attorney general before a hearing. The testimony he gave was hard to understand, incredible in a sense -- to say that he was not involved in discussions and not involved in deliberations, when his three top deputies said he was and the documentary evidence supported that.

It is the decision of Mr. Gonzales as to whether he stays or goes. But it is hard to see how the Department of Justice can function and perform its important duties with Mr. Gonzales remaining where he is. And beyond Mr. Gonzales's decision, it's a matter for the president as to whether the president will retain the attorney general or not.

I think that the operation of the executive branch is a decision for the president. I don't want him telling me how to vote in the Senate on separation of powers, and I'm not going to tell him or make a recommendation to him as to what he ought to do with Mr. Gonzales.

SPECTER: But I think the resignation of Mr. McNulty is another significant step and evidence that a department really cannot function with the continued leadership or lack of leadership of Attorney General Gonzales.

As I view the situation, we really don't know yet what has happened, whether it is politicization or whether it is an ideological bent or what. There is no doubt that the president has the authority to fire all the attorneys general -- pardon me -- in order to fire the attorney general; Freudian slips are sometimes more revealing than the planned statements.

The president does have the authority to replace all of the 93 U.S. attorneys, as President Clinton did when he took office.

And prosecutions for voter fraud are very, very important. When I was district attorney of Philadelphia, I prosecuted both Republicans and Democrats for voter fraud: have a lot of it in Philadelphia.

In 1972, the Democrats and Republicans made a deal in South Philadelphia, a spot where many deals are made, to give the Republicans the top of the ticket -- President Nixon running for reelection -- and the Democrats the rest of the ticket.

A common pleas judge signed in at city hall at 6 a.m. that morning as evidenced by the registry roll, issued injunctions barring all of the McGovern poll watchers from the polling places. He was prosecuted, as were many other top city officials.

So, voter fraud prosecutions are very, very important.

SPECTER: But you can't bring a prosecution unless you have a case.

And now we have to determine if there was chicanery, whether there were efforts at voter prosecutions -- vote fraud prosecutions for investigations when there was no basis for doing so.

It may well be that when we get to the end of the rainbow we will find the explanation may be as simple as outright incompetence -- outright incompetence. To consider firing Peter Fitzgerald, which is what Kyle Sampson testified to, is patently ridiculous.

It is my hope that we will finish these investigations soon, because the continuing investigations are a harm to the -- we have to do our job. But the sooner we finish, the sooner the Department of Justice can return to its work.

If we had a new attorney general and concluded this investigation, made our findings public, it would be very important. Because those U.S. attorneys perform enormously important functions on fighting drugs and crime and terrorism and the administration of both civil and criminal justice in this country.

And I'm glad to see you're here today, Mr. Comey, because I know you can shed some additional light on this important subject.

Thank you, Mr. Chairman.

SCHUMER: Thank you, Senator Specter.

It's now my privilege to introduce our witness today, James B. Comey.

He is almost a man who needs no introduction. He's well known to this committee, which has twice favorably considered his nomination for important offices: first for the U.S. attorney in the Southern District of New York in 2002, then as deputy attorney general of the United States in 2003.

SCHUMER: Mr. Comey was educated at the College of William and Mary and the University of Chicago Law School. After law school, he served as a law clerk for then-U.S. District Judge John M. Walker Jr. in Manhattan. After that he spent most of the next 20 years as a dedicated public servant in the Justice Department.

Besides serving ably as U.S. attorney and deputy attorney general, Mr. Comey earned a reputation as a hard-nosed prosecutor in a number of high-profile and important cases, including Khobar Towers terrorist bombing case arising out of the June 1996 attack on a U.S. military facility in Saudi Arabia in which 19 airmen were killed.

Mr. Comey is currently the senior vice president and general counsel of the Lockheed Martin Corporation.

Now, I know it is not easy for you, Mr. Comey, to be here and talk about some of the recent travails at the department which you hold so dear.

I especially appreciate Mr. Comey's coming to testify here without the formality of a subpoena. In order to secure Mr. Comey's presence, I would have moved for consideration of a subpoena by the committee, but I'm glad that wasn't necessary because of your cooperation.

As far as I'm concerned, when the Justice Department lost Jim Comey, it lost a towering figure. And I don't say that because he stands 6'8" tall.

When Jim left the department, we lost a public servant of the first order, a man of unimpeachable integrity, honestly, character and independence.

And now I'd like to administer the oath of office. Would you please rise?

I sorry. I wish we were administering the oath of office.

(LAUGHTER)

The oath.

Do you affirm that the testimony you are about to give before the committee will be the truth, the whole truth and nothing but the truth so help you, God?

COMEY: I do.

SCHUMER: Thank you.

OK, we're going to get right into the questioning because Mr. Comey does not have an opening statement.

SCHUMER: As I said in my opening remarks, many have been concerned that Alberto Gonzales has made the Justice Department a mere extension of the White House where independence takes a back seat to service to the White House, where the rule of law takes a back seat to the political needs of the president's party.

Before we get to the other issues, I want to go back to an incident from the time that Mr. Gonzales served as White House counsel.

There have been media reports describing a dramatic visit by Alberto Gonzales and Chief of Staff Andrew Card to the hospital bed of John Ashcroft in March 2004, after you, as acting attorney general, decided not to authorize a classified program.

First, can you confirm that a night-time hospital visit took place?

COMEY: Yes, I can.

SCHUMER: OK.

Can you remember the date and the day?

COMEY: Yes, sir, very well. It was Wednesday, March the 10th, 2004.

SCHUMER: And how do you remember that date so well?

COMEY: This was a very memorable period in my life; probably the most difficult time in my entire professional life. And that night was probably the most difficult night of my professional life. So it's not something I'd forget.

SCHUMER: Were you present when Alberto Gonzales visited Attorney General Ashcroft's bedside?

COMEY: Yes.

SCHUMER: And am I correct that the conduct of Mr. Gonzales and Mr. Card on that evening troubled you greatly?

COMEY: Yes.

SCHUMER: OK.

Let me go back and take it from the top.

You rushed to the hospital that evening. Why?

COMEY: I'm only hesitating because I need to explain why.

SCHUMER: Please. I'll give you all the time you need, sir.

COMEY: I've actually thought quite a bit over the last three years about how I would answer that question if it was ever asked, because I assumed that at some point I would have to testify about it.

The one thing I'm not going to do and be very, very careful about is, because this involved a classified program, I'm not going to get anywhere near classified information. I also am very leery of, and will not, reveal the content of advice I gave as a lawyer, the deliberations I engaged in. I think it's very important for the Department of Justice that someone who held my position not do that.

SCHUMER: In terms of privilege.

COMEY: Yes, sir.

SCHUMER: Understood.

COMEY: Subject to that, I -- and I'm uncomfortable talking about this...

SCHUMER: I understand.

COMEY: ... but I'll answer the question.

I -- to understand what happened that night, I, kind of, got to back up about a week.

SCHUMER: Please.

COMEY: In the early part of 2004, the Department of Justice was engaged -- the Office of Legal Counsel, under my supervision -- in a reevaluation both factually and legally of a particular classified program. And it was a program that was renewed on a regular basis, and required signature by the attorney general certifying to its legality.

And the -- and I remember the precise date. The program had to be renewed by March the 11th, which was a Thursday, of 2004. And we were engaged in a very intensive reevaluation of the matter.

And a week before that March 11th deadline, I had a private meeting with the attorney general for an hour, just the two of us, and

I laid out for him what we had learned and what our analysis was in this particular matter.

And at the end of that hour-long private session, he and I agreed on a course of action. And within hours he was stricken and taken very, very ill...

SCHUMER: (inaudible) You thought something was wrong with how it was being operated or administered or overseen.

COMEY: We had -- yes. We had concerns as to our ability to certify its legality, which was our obligation for the program to be renewed.

The attorney general was taken that very afternoon to George Washington Hospital, where he went into intensive care and remained there for over a week. And I became the acting attorney general.

And over the next week -- particularly the following week, on Tuesday -- we communicated to the relevant parties at the White House and elsewhere our decision that as acting attorney general I would not certify the program as to its legality and explained our reasoning in detail, which I will not go into here. Nor am I confirming it's any particular program.

That was Tuesday that we communicated that.

COMEY: The next day was Wednesday, March the 10th, the night of the hospital incident. And I was headed home at about 8 o'clock that evening, my security detail was driving me. And I remember exactly where I was -- on Constitution Avenue -- and got a call from Attorney General Ashcroft's chief of staff telling me that he had gotten a call...

SCHUMER: What's his name?

COMEY: David Ayers.

That he had gotten a call from Mrs. Ashcroft from the hospital. She had banned all visitors and all phone calls. So I hadn't seen him or talked to him because he was very ill.

And Mrs. Ashcroft reported that a call had come through, and that as a result of that call Mr. Card and Mr. Gonzales were on their way to the hospital to see Mr. Ashcroft.

SCHUMER: Do you have any idea who that call was from?

COMEY: I have some recollection that the call was from the president himself, but I don't know that for sure. It came from the White House. And it came through and the call was taken in the hospital.

So I hung up the phone, immediately called my chief of staff, told him to get as many of my people as possible to the hospital immediately. I hung up, called Director Mueller and -- with whom I'd been discussing this particular matter and had been a great help to me over that week -- and told him what was happening. He said, "I'll meet you at the hospital right now."

Told my security detail that I needed to get to George Washington Hospital immediately. They turned on the emergency equipment and drove very quickly to the hospital.

I got out of the car and ran up -- literally ran up the stairs with my security detail.

SCHUMER: What was your concern? You were in obviously a huge hurry.

COMEY: I was concerned that, given how ill I knew the attorney general was, that there might be an effort to ask him to overrule me when he was in no condition to do that.

SCHUMER: Right, OK.

COMEY: I was worried about him, frankly.

And so I raced to the hospital room, entered. And Mrs. Ashcroft was standing by the hospital bed, Mr. Ashcroft was lying down in the bed, the room was darkened. And I immediately began speaking to him, trying to orient him as to time and place, and try to see if he could focus on what was happening, and it wasn't clear to me that he could. He seemed pretty bad off.

SCHUMER: At that point it was you, Mrs. Ashcroft and the attorney general and maybe medical personnel in the room. No other Justice Department or government officials.

COMEY: Just the three of us at that point.

I tried to see if I could help him get oriented. As I said, it wasn't clear that I had succeeded.

I went out in the hallway. Spoke to Director Mueller by phone. He was on his way. I handed the phone to the head of the security detail and Director Mueller instructed the FBI agents present not to allow me to be removed from the room under any circumstances. And I went back in the room.

I was shortly joined by the head of the Office of Legal Counsel assistant attorney general, Jack Goldsmith, and a senior staffer of mine who had worked on this matter, an associate deputy attorney general.

So the three of us Justice Department people went in the room. I sat down...

SCHUMER: Just give us the names of the two other people.

COMEY: Jack Goldsmith, who was the assistant attorney general, and Patrick Philbin, who was associate deputy attorney general.

I sat down in an armchair by the head of the attorney general's bed. The two other Justice Department people stood behind me. And Mrs. Ashcroft stood by the bed holding her husband's arm. And we waited.

And it was only a matter of minutes that the door opened and in walked Mr. Gonzales, carrying an envelope, and Mr. Card. They came over and stood by the bed. They greeted the attorney general very briefly. And then Mr. Gonzales began to discuss why they were there -- to seek his approval for a matter, and explained what the matter was -- which I will not do.

And Attorney General Ashcroft then stunned me. He lifted his head off the pillow and in very strong terms expressed his view of the matter, rich in both substance and fact, which stunned me -- drawn from the hour-long meeting we'd had a week earlier -- and in very strong terms expressed himself, and then laid his head back down on the pillow, seemed spent, and said to them, "But that doesn't matter, because I'm not the attorney general."

SCHUMER: But he expressed his reluctance or he would not sign the statement that they -- give the authorization that they had asked, is that right?

COMEY: Yes.

And as he laid back down, he said, "But that doesn't matter, because I'm not the attorney general. There is the attorney general," and he pointed to me, and I was just to his left.

The two men did not acknowledge me. They turned and walked from the room. And within just a few moments after that, Director Mueller arrived. I told him quickly what had happened. He had a brief -- a memorable brief exchange with the attorney general and then we went outside in the hallway.

SCHUMER: OK.

Now, just a few more points on that meeting.

First, am I correct that it was Mr. Gonzales who did just about all of the talking, Mr. Card said very little?

COMEY: Yes, sir.

SCHUMER: OK.

And they made it clear that there was in this envelope an authorization that they hoped Mr. Ashcroft -- Attorney General Ashcroft would sign.

COMEY: In substance. I don't know exactly the words, but it was clear that's what the envelope was.

SCHUMER: And the attorney general was -- what was his condition? I mean, he had -- as I understand it, he had pancreatitis. He was very, very ill; in critical condition, in fact.

COMEY: He was very ill. I don't know how the doctors graded his condition. This was -- this would have been his sixth day in intensive care. And as I said, I was shocked when I walked in the room and very concerned as I tried to get him to focus.

SCHUMER: Right.

OK. Let's continue.

What happened after Mr. Gonzales and Card left? Did you have any contact with them in the next little while?

COMEY: While I was talking to Director Mueller, an agent came up to us and said that I had an urgent call in the command center, which was right next door. They had Attorney General Ashcroft in a hallway by himself and there was an empty room next door that was the command center.

And he said it was Mr. Card wanting to speak to me.

COMEY: I took the call. And Mr. Card was very upset and demanded that I come to the White House immediately.

I responded that, after the conduct I had just witnessed, I would not meet with him without a witness present.

He replied, "What conduct? We were just there to wish him well."

And I said again, "After what I just witnessed, I will not meet with you without a witness. And I intend that witness to be the solicitor general of the United States."

SCHUMER: That would be Mr. Olson.

COMEY: Yes, sir. Ted Olson.

"Until I can connect with Mr. Olson, I'm not going to meet with you."

He asked whether I was refusing to come to the White House. I said, "No, sir, I'm not. I'll be there. I need to go back to the Department of Justice first."

And then I reached out through the command center for Mr. Olson, who was at a dinner party. And Mr. Olson and the other leadership of the Department of Justice immediately went to the department, where we sat down together in a conference room and talked about what we were going to do.

And about 11 o'clock that night -- this evening had started at about 8 o'clock, when I was on my way home. At 11 o'clock that night, Mr. Olson and I went to the White House together.

SCHUMER: Just before you get there, you told Mr. Card that you were very troubled by the conduct from the White House room (ph), and that's why you wanted Mr. Olson to accompany you.

Without giving any of the details -- which we totally respect in terms of substance -- just tell me why. What did you tell him that so upset you? Or if you didn't tell him just tell us.

COMEY: I was very upset. I was angry. I thought I just witnessed an effort to take advantage of a very sick man, who did not have the powers of the attorney general because they had been transferred to me.

I thought he had conducted himself, and I said to the attorney general, in a way that demonstrated a strength I had never seen before. But still I thought it was improper.

And it was for that reason that I thought there ought to be somebody with me if I'm going to meet with Mr. Card.

SCHUMER: Can you tell us a little bit about the discussion at the Justice Department when all of you convened? I guess it was that night.

COMEY: I don't think it's appropriate for me to go into the substance of it. We discussed what to do. I recall the associate attorney general being there, the solicitor general, the assistant attorney general in charge of the Office of Legal Counsel, senior staff from the attorney general, senior staff of mine. And we just -- I don't want to reveal the substances of those...

SCHUMER: I don't want you to reveal the substance.

They all thought what you did -- what you were doing was the right thing, I presume.

COMEY: I presume. I didn't ask people. But I felt like we were a team, we all understood what was going on, and we were trying to do what was best for the country and the Department of Justice. But it was a very hard night.

SCHUMER: OK.

And then did you meet with Mr. Card?

COMEY: I did. I went with Mr. Olson driving -- my security detail drove us to the White House. We went into the West Wing. Mr. Card would not allow Mr. Olson to enter his office. He asked Mr. Olson to please sit outside in his sitting area. I relented and went in to meet with Mr. Card alone. We met, had a discussion, which was much more -- much calmer than the discussion on the telephone.

After -- I don't remember how long, 10 or 15 minutes -- Mr. Gonzales arrived and brought Mr. Olson into the room. And the four of us had a discussion.

SCHUMER: OK.

And was Mr. -- were you and Mr. Card still in a state of anger at one another at that meeting, or is it a little calmer, and why?

COMEY: Not that we showed.

SCHUMER: Right.

COMEY: It was much more civil than our phone conversation, much calmer.

SCHUMER: Why? Why do you think?

COMEY: I don't know. I mean, I had calmed down a little bit. I'd had a chance to talk to the people I respected. Ted Olson I respect enormously.

SCHUMER: Right. OK.

Was there any discussion of resignations with Mr. Card?

COMEY: Mr. Card was concerned that he had heard reports that there were to be a large number of resignations at the Department of Justice.

SCHUMER: OK. OK.

And the conversations, the issue, whatever it was, was not resolved.

COMEY: Correct. We communicated about it. I communicated again the Department of Justice's view on the matter. And that was it.

SCHUMER: Right.

And you stated that the next day, Thursday, was the deadline for reauthorization of the program, is that right?

COMEY: Yes, sir.

SCHUMER: OK.

Can you tell us what happened the next day?

COMEY: The program was reauthorized without us and without a signature from the Department of Justice attesting as to its legality. And I prepared a letter of resignation, intending to resign the next day, Friday, March the 12th.

SCHUMER: OK.

And that was the day, as I understand it, of the Madrid train bombings.

COMEY: Thursday, March 11th, was the morning of the Madrid train bombings.

SCHUMER: And so, obviously, people were very concerned with all of that.

COMEY: Yes. It was a very busy day in the counterterrorism aspect.

SCHUMER: Yet, even in light of that, you still felt so strongly that you drafted a letter of resignation.

COMEY: Yes.

SCHUMER: OK.

And why did you decide to resign?

COMEY: I just believed...

SCHUMER: Or to offer your resignation, is a better way to put it?

COMEY: I believed that I couldn't -- I couldn't stay, if the administration was going to engage in conduct that the Department of Justice had said had no legal basis. I just simply couldn't stay.

SCHUMER: Right. OK.

Now, let me just ask you this. And this obviously is all troubling.

As I understand it, you believed that others were also prepared to resign, not just you, is that correct?

COMEY: Yes.

SCHUMER: OK.

Was one of those Director Mueller?

COMEY: I believe so. You'd have to ask him, but I believe so.

SCHUMER: You had conversations with him about it.

COMEY: Yes.

SCHUMER: OK.

How about the associate attorney general, Robert McCallum?

COMEY: I don't know. We didn't discuss it.

SCHUMER: How about your chief of staff?

COMEY: Yes. He was certainly going to go when I went.

SCHUMER: Right.

How about Mr. Ashcroft's chief of staff?

COMEY: My understanding was that he would go as well.

SCHUMER: And how...

COMEY: I should say...

SCHUMER: Please.

COMEY: ... to make sure I'm accurate, I...

SCHUMER: This is your surmise, not...

COMEY: Yes.

I ended up agreeing -- Mr. Ashcroft's chief of staff asked me something that meant a great deal to him, and that is that I not resign until Mr. Ashcroft was well enough to resign with me. He was very concerned that Mr. Ashcroft was not well enough to understand fully what was going on. And he begged me to wait until -- this was Thursday that I was making this decision -- to wait til Monday to give him the weekend to get oriented enough so that I wouldn't leave him behind, was his concern.

SCHUMER: And it was his view that Mr. Ashcroft was likely to resign as well?

COMEY: Yes.

SCHUMER: So what did you do when you heard that?

COMEY: I agreed to wait. I said that what I would do is -- that Friday would be last day. And Monday morning I would resign.

SCHUMER: OK.

Anything else of significance relevant to this line of questioning occur on Thursday the 11th, that you can recall?

COMEY: No, not that I recall.

SCHUMER: Thank you.

Now, let's go to the next day, which was March 12. Can you tell us what happened then?

COMEY: I went to the Oval Office -- as I did every morning as acting attorney general -- with Director Mueller to brief the president and the vice president on what was going on on Justice Department's counterterrorism work.

We had the briefing. And as I was leaving, the president asked to speak to me, took me in his study and we had a one-on-one meeting for about 15 minutes -- again, which I will not go into the substance of. It was a very full exchange. And at the end of that meeting, at my urging, he met with Director Mueller, who was waiting for me downstairs.

He met with Director Mueller again privately, just the two of them. And then after those two sessions, we had his direction to do the right thing, to do what we...

SCHUMER: Had the president's direction to do the right thing?

COMEY: Right.

We had the president's direction to do what we believed, what the Justice Department believed was necessary to put this matter on a footing where we could certify to its legality.

And so we then set out to do that. And we did that.

SCHUMER: OK.

So let me just (inaudible) -- this is an amazing story, has an amazing pattern of fact that you recall.

SPECTER: Mr. Chairman, could you give us some idea when your first round will conclude?

SCHUMER: As soon as I ask a few questions here. Fairly soon.

(OFF-MIKE)

SCHUMER: Yes.

And, Senator Specter, you will get the same amount of time.

SCHUMER: I thought with Mr. Comey's telling what happened...

(CROSSTALK)

SPECTER: Just may the record show that you're now 16 minutes and 35 seconds over the five minutes and...

SCHUMER: I think the record will show it.

SPECTER: Well, it does now.

(LAUGHTER)

SCHUMER: OK, thank you.

And I think most people would think that those 16:35 minutes were worth hearing.

SPECTER: Well, Mr. Chairman, we do have such a thing as a second round, and there are a lot of senators waiting...

SCHUMER: Yes, OK.

Let me ask you these few questions...

SPECTER: ... including a Republican.

SCHUMER: I'm glad you're here, Senator Specter. I know you're concerned with the issue.

SPECTER: Lonely, but here.

(LAUGHTER)

SCHUMER: Let me ask you this: So in sum, it was your belief that Mr. Gonzales and Mr. Card were trying to take advantage of an ill and maybe disoriented man to try and get him to do something that many, at least in the Justice Department, thought was against the law? Was that a correct summation?

COMEY: I was concerned that this was an effort to do an end-run around the acting attorney general and to get a very sick man to approve something that the Department of Justice had already concluded -- the department as a whole -- was unable to be certified as to its legality. And that was my concern.

SCHUMER: OK.

And you also believe -- and you had later conversations with Attorney General Ashcroft when he recuperated, and he backed your view?

COMEY: Yes, sir.

SCHUMER: Did you ever ask him explicitly if he would have resigned had it come to that?

COMEY: No.

SCHUMER: OK.

But he backed your view over that what was being done, or what was attempting to being done, going around what you had recommended, was wrong, against the law?

COMEY: Yes.

And I already knew his view from the hour we had spent together going over it in great detail a week before the hospital incident.

SCHUMER: Yes.

And the FBI director, Mueller, backed your view over that of Mr. Gonzales as well -- is that right? -- in terms of whether the program could continue to be implemented the way Counsel Gonzales wanted it to be.

COMEY: The only reason I hesitate is it was never Director Mueller's job or position to be drawing a legal conclusion about the program; that he was very supportive to me personally. He's one of the finest people I've ever met and was a great help to me when I felt a tremendous amount of pressure and felt a bit alone at the Department of Justice.

But it was not his role to opine on the legality.

SCHUMER: How about Jack Goldsmith, the head of the Office of Legal Counsel? Did he opine on the legality?

COMEY: Yes. He had done a substantial amount of work on that issue. And it was largely OLC, the Office of Legal Counsel's work, that I was relying upon in drawing my -- in making my decision.

SCHUMER: OK. Just two other questions.

Have you ever had the opportunity to recall these events on the record in any other forum?

COMEY: No.

SCHUMER: OK. And...

COMEY: I should...

SCHUMER: Go ahead.

COMEY: I was interviewed by the FBI and discussed these events in connection with a leak investigation the FBI was conducting.

SCHUMER: And you gave them these details then.

COMEY: Yes.

SCHUMER: Thank you.

COMEY: But not -- by forum I've never testified about it.

SCHUMER: And after you stood your ground in March of 2004, did you suffer any recriminations or other problems at the department?

COMEY: I didn't. Not that I'm aware of.

SCHUMER: OK.

Well, let me just say this, and then I'll call on Senator Specter who can have as much time as he thinks is appropriate.

The story is a shocking one. It makes you almost gulp.

And I just want to say, speaking for myself, I appreciate your integrity and fidelity to rule of law. And I also appreciate Attorney General Ashcroft's fidelity to the rule of law as well, as well as the men and women who worked with you and stuck by you in this.

When we have a situation where the laws of this country -- the rules of law of this country are not respected because somebody thinks there's a higher goal, we run askew of the very purpose of what democracy and rule of law are about.

SCHUMER: And this -- again, this story makes me gulp.

Senator Specter?

SPECTER: May the record now show that we're 21 minutes and 22 seconds beyond the five-minute allocation.

And I raise it not to in any way suggest that the questioning hasn't been very important, but only to suggest that we have a practice for having a five-minute round. And it is exceeded on some occasions. I've only been here 27 years; I can't remember it being exceeded by about 23 minutes.

And we do have second rounds. And we do have eight -- seven Democrats here. It is now 9:48 -- 10:48. And at the start of this hearing I asked my colleagues among the Republicans to join me here.

I repeat that request now, since it's televised -- internally, at least -- that my colleagues should know that there are seven Democrats here who will all have turns asking questions. And it would be appropriate to have a little balance here, if some Republicans would show up to participate in this hearing. It would be helpful if we had some balance, if some other Republicans would show up to participate in this hearing.

Mr. Comey, I join Senator Schumer in commending you for what you did here. The terrorist surveillance program has been the subject of quite a number of hearings in this committee: strenuous efforts to bring the issue before the Foreign Intelligence Surveillance Court, efforts at changing legislation; some of it is now pending, co-sponsored by Senator Feinstein and myself. The matter is wending its way through the federal courts, and it's the 6th Circuit now.

So this is a very important, substantive matter.

SPECTER: And as the acting attorney general, you were doing exactly what you should do in standing up for your authority and to stand by your guns and to do what you thought was right.

It has some characteristics of the Saturday Night Massacre, when the other officials stood up and they had to be fired in order to find someone who would -- deputy attorney general and others would not fire the special prosecutor. So that was commendable.

When you finally got to the place where the buck doesn't stop, when you got to the president -- as I understand your testimony -- the president told you to do what you thought was right. Is that correct?

COMEY: Yes, sir.

SPECTER: So the president backed you up. And it was necessary to make changes in the terrorist surveillance program to get the requisite certification by the acting attorney general -- that is you?

COMEY: And I may be being overly cautious, but I'm not comfortable confirming what program it was that this related to.

And I should be clear. The direction -- as I said, I met with the president first, the Director Mueller did.

COMEY: And it was Director Mueller who carried to me the president's direction to do what the Department of Justice thinks is right to get this where the department believes it ought to be. And we acted on that direction.

SPECTER: Director Mueller told you to -- the president said to do what you thought was right?

COMEY: Correct.

SPECTER: Well, how about what the president himself told you?

COMEY: I don't want to get into what -- the reason I hesitate, Senator Specter, is the right thing was done here, in part -- in large part because the president let somebody like me and Bob Mueller meet with him alone.

And if I talk about that meeting, I worry that the next president who encounters this is not going to let the next me get close to them to talk about something this important.

So I'm -- I want to be very careful that I don't talk about what the president and I talked about.

I met with the president. We had a full and frank discussion, very informed. He was very focused.

Then Director Mueller met with the president alone. I wasn't there.

Director Mueller carried to me the president's direction that we do what the Department of Justice wanted done to put this on a sound legal footing.

SPECTER: So you met first with the president alone for 15 minutes?

COMEY: Yes, sir.

SPECTER: And then Director Mueller met separately with the president for 15 minutes?

COMEY: I don't remember exactly how long it was. It was about the same length as my meeting. I went down and waited for him, as he...

SPECTER: And then Director Mueller, as you've testified, said to you, the president told Director Mueller to tell you to do what the Department of Justice thought was right?

COMEY: Correct.

SPECTER: Well -- but you won't say whether the president told you to do what the Department of Justice said was right?

COMEY: Yes, I...

SPECTER: You're not slicing hair. There's no hair there.

COMEY: You're a good examiner.

And that...

SPECTER: Well, thank you.

COMEY: Yes. I -- the president and I -- I don't think the conversation was finished. We discussed the matter in some detail. And then I urged him to talk to Bob Mueller about it.

And I don't know the content of Director Mueller's communication with him, except that Director Mueller -- the president didn't give me that -- I can answer that question.

The president didn't give me that direction at the end of our 15 minutes.

SPECTER: He did not?

COMEY: He did not. Instead, he said, "I'll talk to Director Mueller," as I had suggested.

Director Mueller came and met with him, then Director Mueller came to me and said that, "The president told me that the Department of Justice should get this where it wants to be, to do what the department thinks is right."

And I took that mandate and set about to do that, and accomplished that.

SPECTER: I thought you testified, in response to Senator Schumer's questions, that after meeting with the president for 15 minutes, he told you to do what you thought was right.

COMEY: If I did, I misspoke, because that direction came from the president to Director Mueller to me.

SPECTER: Well, when you had the discussions with Chief of Staff Card, what did he say to you by way of trying to pressure you, if, in fact, he did try to pressure you, to give the requisite certification?

COMEY: Again, I'm reluctant to talk about the substance of those kind of deliberative discussions. We discussed...

SPECTER: And I'm not asking about the substance, carefully not. I'm going to, but not yet.

What did he say which constituted what you thought was pressure?

COMEY: I don't know that he tried to pressure me, other than to engage me on the merits and to make clear his strong disagreement with my conclusion.

SPECTER: So then Mr. Card ultimately left it up to you to decide whether to give the certification or not?

COMEY: I don't know that he left it up to me. I had already made a decision and communicated it on that Tuesday, that I was not going to. And it didn't change in the course of my discussions with Mr. Card.

SPECTER: Did not change?

COMEY: Did not change.

SPECTER: Well, he didn't threaten to fire you, did he? I'm going to have to lead the witness now, Mr. Comey.

COMEY: Right.

SPECTER: I'm -- I haven't led you up until now. And now I'm going to have to lead you.

COMEY: That's fine.

SPECTER: He didn't threaten to fire you?

COMEY: No, he didn't.

And Mr. Card, as I said, was very civil to me in our face-to-face meeting. The only time...

SPECTER: Well, you can suggest being fired and be civil about it.

COMEY: Right.

Either civilly or uncivilly, he never suggested that to me.

SPECTER: Attorney General Gonzales could be fired in a civil way. No incivility in suggesting you're going to be replaced as acting attorney general.

Well, all right then. That substance -- I don't want to question you as long as Senator Schumer did, notwithstanding my rights here. But the long and short of it was, he didn't threaten you.

COMEY: No, sir. I didn't feel threatened. Nor did he say anything that I thought could reasonably be read...

SPECTER: And when you talked to White House Counsel Gonzales, did he try to pressure you to reverse your judgment?

COMEY: No.

He disagreed, again, on the merits of the decision. And we had engaged on that, had full discussions about that.

But he never tried to pressure me, other than to convince me that I was wrong.

SPECTER: Well, Mr. Comey, did you have discussions with anybody else in the administration who disagreed with your conclusions?

COMEY: Yes, sir.

SPECTER: Who else?

COMEY: Vice president.

SPECTER: Anybody else?

COMEY: Members of his staff.

SPECTER: Who on his staff?

COMEY: Mr. Addington disagreed with the conclusion. And I'm sure there were others who disagreed, but...

SPECTER: Well, I don't want to know who disagreed. I want to know who told you they disagreed.

COMEY: OK.

SPECTER: Addington?

COMEY: Mr. Addington. The vice president told me that he disagreed. I don't remember any other White House officials telling me they disagreed.

SPECTER: OK. So you've got Card, Gonzales, Vice President Cheney and Addington who told you they disagreed with you.

COMEY: Yes, sir.

SPECTER: Did the vice president threaten you?

COMEY: No, sir.

SPECTER: Did Addington threaten you?

COMEY: No, sir.

SPECTER: So all these people told you they disagreed with you?

Well, why in this context, when they say they disagreed with you and you're standing by your judgment, would you consider resigning? You were acting attorney general. They could fire you if they wanted to. The president could replace you. But why consider resigning?

You had faced up to Card and Gonzales and Vice President Cheney and Addington, had a difference of opinion. You were the acting attorney general, and that was that. Why consider resigning?

COMEY: Not because of the way I was treated but because I didn't believe that as the chief law enforcement officer in the country I could stay when they had gone ahead and done something that I had said I could find no legal basis for.

SPECTER: When they said you could find no legal basis for?

COMEY: I had reached a conclusion that I could not certify as...

SPECTER: Well, all right, so you could not certify it, so you did not certify it.

But why resign? You're standing up to those men. You're not going to certify it. You're the acting attorney general. That's that.

COMEY: Well, a key fact is that they went ahead and did it without -- the program was reauthorized without my signature and without the Department of Justice. And so I believed that I couldn't stay...

SPECTER: Was the program reauthorized without the requisite certification by the attorney general or acting attorney general?

COMEY: Yes.

SPECTER: So it went forward illegally.

COMEY: Well, that's a complicated question. It went forward without certification from the Department of Justice as to its legality.

SPECTER: But the certification by the Department of Justice as to legality was indispensable as a matter of law for the program to go forward, correct?

COMEY: I believed so.

SPECTER: Then it was going forward illegally.

COMEY: Well, the only reason I hesitate is that I'm no presidential scholar.

But if a determination was made by the head of the executive branch that some conduct was appropriate, that determination -- and lawful -- that determination was binding upon me, even though I was the acting attorney general, as I understand the law.

And so, I either had to go along with that or leave. And I believed that I couldn't stay -- and I think others felt this way as well -- that given that something was going forward that we had said we could not certify as to its legality.

SPECTER: Well, I can understand why you would feel compelled to resign in that context, once there had been made a decision by the executive branch, presumably by the president or by the president, because he was personally involved in the conversations, that you would resign because something was going forward which was illegal.

The point that I'm trying to determine here is that it was going forward even though it was illegal.

COMEY: And I know I sound like I'm splitting hairs, but...

SPECTER: No, I don't think there's a hair there.

COMEY: Well, something was going forward without the Department of Justice's certification as to its legality. It's a very complicated matter, and I'm not going to go into what the program was or what the dimensions of the program...

SPECTER: Well, you don't have to.

If the certification by the Department of Justice as to legality is required as a matter of law, and that is not done, and the program goes forward, it's illegal. How can you -- how can you contest that, Mr. Comey?

COMEY: The reason I hesitate is I don't know that the Department of Justice's certification was required by statute -- in fact, it was not, as far as I know -- or by regulation, but that it was the practice in this particular program, when it was renewed, that the attorney general sign off as to its legality.

There was a signature line for that. And that was the signature line on which was adopted for me, as the acting attorney general, and that I would not sign.

So it wasn't going forward in violation of any -- so far as I know -- statutory requirement that I sign off. But it was going forward even though I had communicated, "I cannot approve this as to its legality."

And given that, I just -- I couldn't, in good conscience, stay.

SPECTER: Well, Mr. Comey, on a matter of this importance, didn't you feel it necessary to find out if there was a statute which required your certification or a regulation which required your certification or something more than just a custom?

COMEY: Yes, Senator. And I...

SPECTER: Did you make that determination?

COMEY: Yes, and I may have understated my knowledge. I'm quite certain that there wasn't a statute or regulation that required it, but that it was the way in which this matter had operated since the beginning.

I don't -- I think the administration had sought the Department of Justice, the attorney general's certification as to form and legality, but that I didn't know, and still don't know, the source for that required in statute or regulation.

SPECTER: OK. Then it wasn't illegal.

COMEY: That's why I hesitated when you used the word "illegal."

SPECTER: Well, well, OK.

Now I want your legal judgment. You are not testifying that it was illegal. Now, as you've explained that there's no statute or regulation, but only a matter of custom, the conclusion is that even though it violated custom, it is not illegal.

It's not illegal to violate custom, is it?

COMEY: Not so far as I'm aware.

SPECTER: OK. So what the administration, executive branch of the president, did was not illegal.

COMEY: I'm not saying -- again, that's why I kept avoiding using that term. I had not reached a conclusion that it was.

The only conclusion I reached is that I could not, after a whole lot of hard work, find an adequate legal basis for the program.

SPECTER: OK.

Well, now I understand why you didn't say it was illegal. What I don't understand is why you now won't say it was legal.

COMEY: Well, I suppose there's an argument -- as I said, I'm not a presidential scholar -- that because the head of the executive branch determined that it was appropriate to do, that that meant for purposes of those in the executive branch it was legal.

I disagreed with that conclusion. Our legal analysis was that we couldn't find an adequate legal basis for aspects of this matter. And for that reason, I couldn't certify it to its legality.

SPECTER: OK.

I will not ask you -- I have a rule never to ask the same question more than four times...

(LAUGHTER)

... so I will not ask you again whether necessarily from your testimony the conclusion is that what the president did was legal -- not illegal.

Let me move on. I only have 35 minutes left.

(LAUGHTER)

How long did you continue to serve as deputy attorney general after this incident?

COMEY: Until August of 2005, so almost a year and a half, 16 months.

SPECTER: And during the course of that continued service, you got along OK with the president and the vice president and Card and Addington and all the rest of those fellows in the White House?

COMEY: I think so. I mean, we didn't have much contact with them other than professional matters. But I think so.

SPECTER: But they weren't out to get you because you stood out to them?

COMEY: I hope not. I don't have any reason to believe...

SPECTER: Well, never mind hoping. They didn't do anything to be out to get you or to make your life uncomfortable, or make it difficult for you to perform your duties as deputy attorney general?

COMEY: No.

SPECTER: There was some speculation that -- well, I'll eliminate the word "speculation."

Did you have any sense that you were not considered to be permanent attorney general on Mr. Ashcroft's departure because of your having stood up to the White House on this issue?

COMEY: No.

And I don't have any reason to believe I was ever considered. But I certainly have no reason to believe that there was any connection between consideration of who would be the next attorney general and this matter.

SPECTER: Well, on this issue, Mr. Comey, I commend you again. You did exactly the right thing.

SPECTER: And I think the president did the right thing. In effect, he overruled Card and he overruled Vice President Cheney and he overruled Addington and he overruled Gonzales. And when it came to him -- came to the president's desk where the buck stops he said to Mueller to tell you, "Follow your conscience. Do the right thing." And that was that.

Mr. Comey, it's my hope that we will have a closed session with you to pursue the substance of this matter further. Because your standing up to them is very important, but it's also very important what you found on the legal issue on this unnamed subject, which I infer was the terrorist surveillance program. And you're not going to comment about it. I think you could.

I think you could even tell us what the legalisms were. Doesn't involve a matter of your advice or what the president told you, et cetera.

But I'm going to discuss it with Senator Leahy later and see about pursuing that question to try to find out about it.

Now, Mr. Comey, on to the subject of the hearing. You have been reported as commenting on a number of U.S. attorneys who were asked to resign. You thought they were doing a good job. One was U.S. Attorney David (sic) Bogden of Nevada.

What judgment did you -- do you have as to his capabilities as U.S. attorney?

COMEY: Dan Bogden was an excellent U.S. attorney. He was a career guy who had become U.S. attorney, and I thought very highly of him.

SPECTER: Do you have any insights as to why he was asked to resign?

COMEY: I don't. I've read things in the paper, but I certainly have no personal knowledge of why he was asked to resign. When I left in August of 2005, I couldn't have thought of a reason why he should be asked to resign.

SPECTER: And as to John McKay, do you have a judgment as to the quality, the competency of his performance?

COMEY: Yes. Again, it was excellent in my experience. I had worked with him, as with the others, as a peer when I was U.S. attorney in Manhattan and then as the deputy attorney general. So I had a very positive sense of John McKay.

SPECTER: And as to Paul Charlton, Arizona U.S. attorney, what is your view as to his competence?

COMEY: The same. I don't want to make it sound like I love everybody, but I did like him a great deal.

(LAUGHTER)

He was very strong.

SPECTER: Well, since you don't want to sound like you love everybody, anybody you didn't love who you thought should have been replaced?

(LAUGHTER)

LEAHY: Outside of members of the committee.

COMEY: There was one U.S. attorney...

(CROSSTALK)

SPECTER: I'd like to ask you about that now that Senator Leahy has opened the door. Which members of the committee don't you love?

(LAUGHTER)

COMEY: You're asking Senator Leahy, I hope.

SPECTER: Start with the chairman.

(LAUGHTER)

LEAHY: Careful. We may be bringing (ph) the clock back again.

SPECTER: What you think of Charlton?

COMEY: Very strong, very strong U.S. attorney.

SPECTER: And David Iglesias, U.S. attorney for New Mexico?

COMEY: Same thing. I had dealt with him quite a bit, both as a peer and as his supervisor, and had a high opinion of him. I thought he did a very good job.

SPECTER: What did you make of Kyle Sampson's testimony that he had recommended calling for the resignation of Peter Fitzgerald?

COMEY: Of Patrick Fitzgerald.

SPECTER: Patrick Fitzgerald. Peter Fitzgerald was the senator.

(UNKNOWN): No relation.

SPECTER: No relation.

COMEY: I only know about that what I read in the newspaper. I was surprised by it, would be a fair description.

SPECTER: And what did you think of the competency of Kyle Sampson?

COMEY: I thought Kyle was very smart. My dealings with him had always been pleasant. He seemed to work very, very hard.

SPECTER: What did you think of the competency or smarts of Kyle Sampson after you heard he wanted to ask for the resignation of Patrick Fitzgerald?

COMEY: Well, I don't think that was an exercise of good judgment, if it's something he really meant. It...

SPECTER: Can you give us an illustration of an exercise in good judgment by Kyle Sampson?

I withdraw that question.

Can you give us an example of an exercise of good judgment by Alberto Gonzales?

Let the record show a very long pause.

COMEY: It's hard -- I mean, I'm sure there are examples. I'll think of some.

I mean, it's hard when you look back. We worked together for eight months.

SPECTER: That's a famous statement of President Eisenhower about Vice President Nixon: "Say something good." "Give me two weeks."

COMEY: Right.

I -- in my experience with Attorney General Gonzales, he was smart and engaged. And I had no reason to question his judgment during our time together at the Department of Justice.

We had a good working relationship. He seemed to get issues. I would make a recommendation to him. He would discuss it with me and make a decision.

As I sit here today, I'll probably five minutes from now think of an example. But I did not have reason to question his judgment as attorney general.

SPECTER: Are you sufficiently familiar with what happened in the issue of the U.S. attorneys resignations to give an evaluation of Attorney General Gonzales' statement that he was no involved in discussions or deliberations, in the context of being contradicted by three of his top deputies and the documentary evidence on the e-mails?

COMEY: I am probably more versed in this than the average person, because I've read what's in the newspaper and looked at some of the documents online.

But I gather he's corrected that statement that he originally made about not being involved in deliberations or discussions.

But I'm not -- I don't know the facts as well as members of this committee, and haven't studied it. So I don't think I have a...

SPECTER: No, I don't think he has corrected that. I think he continues to say that he was involved in a -- his words are "limited" -- quote, "limited," unquote.

SPECTER: That's what he has said.

I think that -- and I've said this to Mr. Gonzales privately and publicly -- that if he would tell us what the reasons were for asking these U.S. attorneys to resign, that it would shed considerable light on what's going on here, on how the program got started, and what the aims of the program were, and what his involvement was.

That can -- that can all be -- this proceeding is still in midstream. He can recant all of what he's said and come forward.

Well, Mr. Chairman, I'm going to yield the balance of my minutes. Thank you.

SCHUMER: Thank you, Mr. Chairman. And you went about, I think, a minute more than I did.

SPECTER: Oh, no I didn't. I'm at 21:35.

SCHUMER: OK. I just...

LEAHY: So we can get on to others, I'm also -- as a member of this committee, let me just go back to the time. I'm not going to use a great deal of time so that...

SPECTER: Senator Schumer and I didn't either, Senator Leahy.

LEAHY: ... so that -- God love you -- so that others here can.

Just one question comes to mind.

Senator Specter spoke to you about legal or illegal. Did it comply with the FISA law?

COMEY: If I -- I've tried, Senator, not to confirm that I'm talking about any particular program. I just don't feel comfortable in an open forum...

LEAHY: OK.

Then on that -- with that answer, I think I agree with -- if I could have Senator Specter's attention just for a moment. With that answer -- and I can understand. I'm well aware of the program, well aware of what happened. And I can understand your reluctance -- very appropriately, your reluctance to answer that specifically.

We will have a closed-door hearing on this. Senator Specter and

I are about to have a briefing on aspects of this.

LEAHY: I am very, very troubled by what the Department of Justice is going today -- not on your watch, Mr. Comey, but they're doing today. We have several members of the Intelligence Committee on this committee on both sides. And they will also be looking at it.

Mr. Comey, I have a lot of respect for you. I have less and less respect for the way the Department of Justice is being handled today. This is a dysfunctional Department of Justice. It is being run like a political arm of the White House. That is highly inappropriate.

I've been here for 32 years. I've seen good attorneys general and poor attorneys general. I have always thought that there would at least be the understanding that the professionals in the Department of Justice have to be allowed to do a professional job. And when I see them being overridden time and time again.

Now, I realize there are some things you cannot go into in this session. But you know and I know that there is the overriding of the professional judgment of good men and women in that department to do things that are not proper. And I think this is wrong.

One of my first experiences in the Department of Justice was as a young law clerk working while a student at Georgetown here meeting with the then-attorney general. The then-attorney general was a close to the president as anyone could. He was his brother. This was Attorney General Robert Kennedy.

But I remember what he said to several of the students who were there, because he was hoping we were a cadre, because of our grades and whatnot, he wanted to recruit for the Department of Justice. And he emphasized over and over again on significant matters -- civil rights, criminal, (inaudible) areas and whatnot -- that neither the White House nor his brother would be allowed to influence the professional judgment.

That always stuck in my mind.

LEAHY: And I've seen that happen over and over again. We saw it with Elliot Richardson and Archibald Cox. We saw it with you.

And I am very, very frustrated. I won't go into further questions, because the questions I do want to ask you will be in closed session.

But I hope -- I hope somebody will wake up at the White House at the terrible, terrible precedent they are starting and have started. And I hope whoever the next president is will make a solemn vow never, never, never to allow this politicization of the Department of Justice. Because it hurts every one of us.

It's not the secretary of justice. It's not a member of the president's staff that should be running that. It is the attorney general of the United States. And this attorney general is doing an abysmal job.

SCHUMER: Thank you, Mr. Chairman.

Senator Kohl?

Senator Feinstein was next. I apologize.

FEINSTEIN: Thank you very much, Mr. Chairman.

And thank you very much, Mr. Comey.

I read the transcript of your testimony before the House. And it's clear that you're a very straight shooter and very well respected. And I, for one, really appreciate your point of view.

If I can, I'd like to go back to the event in the hospital room for just a minute. You felt -- and you were presented with something that you had to sign to certify a certain program. That program was initially done outside of the existing law, which is the Foreign Intelligence Surveillance Act, which provides -- which says it's the exclusive authority for all electronic surveillance.

The president used his Article II powers. He said he used the authorization to use military force as the definitive basis for his action, to essentially move outside the law.

However, you were faced -- and the president said when this all came to light that he asked the program -- asked that the program be authorized every 45 days, or certified by the attorney general.

What did you actually have to sign to certify it? What were you confronted with?

COMEY: Senator, I want to be careful in this forum, again, that I'm not confirming the existence of any particular program or that this dispute...

FEINSTEIN: I'm not asking you to. I'm asking you, what piece of paper did you have to sign?

COMEY: It was a signature line on a presidential order.

FEINSTEIN: OK. All right.

And you said that the program was later changed so that it could be signed. But it went ahead at that time without your certification on it.

COMEY: Yes.

FEINSTEIN: And what was the elapsed period of time from that meeting, the denial of DOJ to certify the program and the time when it was essentially certified?

COMEY: It was reauthorized on Thursday, March the 11th, without the department's -- without my signature, without the department's approval.

And it was the next day -- so less than 24 hours later -- that we received the direction from the president to make it right.

And then we set about -- I don't remember exactly how long it was -- over the next few weeks making changes so that it accorded with our judgment about what could be certified as to legality.

And so it was really only that period from Thursday, when it was reauthorized, until I got the direction from the president the next day that it operated outside the Department of Justice's approval.

FEINSTEIN: For approximately two weeks?

COMEY: I don't remember exactly. It was two or three weeks I think that it took us to get the analysis done and make the changes that needed to be made.

FEINSTEIN: And then who signed for DOJ?

COMEY: It was either the attorney general, Ashcroft, or myself who signed. I may have signed that first one after the hospital incident.

FEINSTEIN: OK.

And you then became satisfied that the program conformed with what, essentially?

COMEY: That it was operated consistently with the Office of Legal Counsel's judgment about what was lawful. So we were in a position -- given OLC's opinion, the attorney general and I were in a position to certify the program as to its legality.

FEINSTEIN: Mr. Chairman, it would be very interesting if we could obtain those legal opinions. Because the program we're talking about was originally done outside of law. The executive order of the president was really the prevailing authority.

But even so, I'm a little puzzled because the program was changed. And I'd be very interested in what the legal advise on that program was if that would be possible for us to request.

SCHUMER: I'm sure if the senator makes the request we can make it part of the record.

FEINSTEIN: Fine, I've made that request...

(CROSSTALK)

SCHUMER: I think to the Office of Legal Counsel, which had already stated its opinion on this particular issue.

(CROSSTALK)

FEINSTEIN: Thank you. Thank you.

If I can, I'd like to move on to the United States attorneys.

To the best of your knowledge, has there been any time in the history of our country when as many U.S. attorneys have been fired at one time?

COMEY: The only other incident I know of was during the change of administrations from Bush I to President Clinton's administration.

FEINSTEIN: Which is fairly typical...

(CROSSTALK)

COMEY: Right, it was a change out...

(CROSSTALK)

FEINSTEIN: With a change. But I'm talking during the term of a president has there been any time when a number of U.S. attorneys had been selected and summarily fired without cause?

COMEY: I'm not aware of a similar-size removal of U.S. attorneys.

FEINSTEIN: Thank you very much.

As you know, we've had the EARS reports. Are you familiar with those reports?

COMEY: Yes.

FEINSTEIN: And they have described the performance of U.S. attorneys -- and I gather there's a panel of people that go in and put these reports together. They have subsequently been -- we've been told that they're very, very perfunctory.

Are they, in fact, a document that's utilized within DOJ?

COMEY: Oh, yes.

(LAUGHTER)

And they're not perfunctory. They come -- big team of people.

When I was U.S. attorney in New York, I think 30 or more people came from all over the country -- experienced people, civil lawyers and prosecutors -- and they basically live with you in your office for a couple of weeks and go stem to stern, inspect the whole place. There's an out-briefing.

It's very much like an audit by a big accounting firm, except they audit not just your numbers, but your conduct of cases and your priorities. So it's from top to bottom, and then they issue a detailed report.

FEINSTEIN: Well, let me ask you this question: How then could they be fired for performance reasons if at least seven -- excuse me -- six out of the seven terminated on December 7th had excellent EARS reports?

COMEY: I don't know. I was not aware at the time I left, in August of 2005, of performance-related issues with most of these U.S. attorneys.

FEINSTEIN: And you've said that. You said that today. You said that in your testimony before the House. And I appreciate it.

Can you ever remember any discussion where an individual U.S. attorney's loyalty or political instincts were questioned?

COMEY: I don't remember ever discussing or having it discussed in my presence the loyalty or political instincts of a U.S. attorney, no.

FEINSTEIN: Now, there was apparently a list put together.

FEINSTEIN: And Mr. Sampson had indicated that he was the aggregator of the list. He put the list together.

But everyone that we've asked in the higher levels of the department have said they did not put the names on the list. Mr. Battle, Mr. Ellston, Mr. Sampson -- virtually everyone we have asked have denied placing a name on that list.

If that is in fact the case, where would you surmise the list would come from?

COMEY: I wouldn't know. It came from someplace, but I don't know from where.

FEINSTEIN: I'd like to just clear the air with one thing.

You had two meetings with Carol Lam, I believe -- one about the Project Neighborhood program, the other about gun cases. Were you satisfied with her responses to your questions?

COMEY: Yes.

I think I had one meeting that was about Project Safe Neighborhoods, which was the name given to our gun program. And I think it was on the telephone. I spoke to -- I think by telephone -- to each of the 10 U.S. attorneys whose districts on a per capita basis were at the bottom end of our gun prosecutions.

And I thought she understood. And, again, I wasn't telling her to do cases for the sake of doing cases. I was saying, "This is important. I think this saves lives. If there's a difference you can make that the local prosecutors are not making in your jurisdiction, look for an opportunity to make it."

And she said she got it. And that was the end of it.

FEINSTEIN: Were any of the other 10 people with whom you communicated fired?

COMEY: No, not to my knowledge.

FEINSTEIN: So if someone had an excellent performance report, it's very difficult for me to figure out a reason other than dissatisfaction with a case they were either going to file or not file if the severance is not performance-related.

Would that be a fair assumption on my part?

COMEY: I suppose so. Right. If there's no reasons that are apparent -- performance-related reasons -- it's hard to understand why.

FEINSTEIN: Thank you very much, Mr. Comey. Appreciate it.

Thank you.

SCHUMER: Senator Kohl?

KOHL: Thank you, Mr. Chairman.

Mr. Comey, you're a person of course who has been very close to law enforcement in our country for many years. And obviously, you're here today as a person who was the second-ranking person in the department from 2003 to 2005.

KOHL: And no question about your concern for the fair administration of justice in our country. And with the kind of experience you have, your opinions matter more than the opinions of most others. And I'm sure you've thought about this; would you give us your opinion?

Would our country be well-served if we could start fresh tomorrow with an attorney general who was not in any way as tainted as this present attorney general? Would we be better off as a country?

You must have an opinion. Would you care to share that opinion with us?

COMEY: I would very much like not to.

(LAUGHTER)

KOHL: But would you, please?

COMEY: I would hope -- there are a lot of things I miss about government. A lot of things I love about being a private citizen.

I would hope you wouldn't care what my opinion is.

I appreciate what you said, Senator. I'm not here to dump on Attorney General Gonzales. I...

KOHL: Well, this isn't a question of jumping on -- we're talking about our country and its future and the importance of law, the importance of the Department of Justice. And you have been closer than most.

And you are here to serve your country; that's why you're here today.

And that's a very important question, obviously. And your opinion matters much more than most, because of who you are and your experience.

And I'm sure, or I presume, you do have an opinion. Would you share that opinion with us today?

COMEY: I do have an opinion. I would prefer not to share it. I'm just not sure that -- it makes me very uncomfortable to express my opinion about something, especially now that I'm outside of government and that I have not followed this as closely as many people have.

I have formulated an opinion, but I would ask the senator's indulgence not to make me give it. I just don't think that's my place.

KOHL: Well, I'm concluding -- and correct me if I'm incorrect -- I'm concluding that your unwillingness to express an opinion that you do say -- you say that you have -- is an indication that you believe we would be better served. I think that's a clear inference from what you're saying.

COMEY: I appreciate that, Senator.

COMEY: If I could, I'd like not to offer that.

KOHL: To me, you have expressed that opinion. I mean, without having expressed it, you expressed it.

Mr. Comey, when you testified in the House a few weeks ago, you were asked about the U.S. attorney for the Eastern District of Wisconsin, Steve Biskupic. At that time, you said that Mr. Biskupic was, quote, "an absolutely straight guy," unquote.

When you were asked whether you knew that Mr. Biskupic was on a list for weak performers and potentially slated for dismissal, you said -- and I quote -- "No, and I think very highly of him."

Having had time to reflect on your testimony, do you have anything to add to what you said at that time? Do you know why he was put on a list of weak performers, and why he came off the list?

Did it have anything to do with the prosecution of voter fraud cases that he was taken off the list, or the prosecution of Georgia Thompson, an employee of the Democratic governor's administration at that time?

COMEY: I don't know from firsthand knowledge that he was on a list. I can't imagine why he would be put on a list (inaudible).

I think very highly of him, as you quoted. I think he is what you want in a U.S. attorney. And I'm not saying that because he's tall and skinny...

(LAUGHTER)

... but he is a very solid person, who is as honest as the day is long, cares passionately about the independence of the Department of Justice. I know this from talking to him.

So I can't imagine -- I know he's gotten beat on because a case he prosecuted was reversed in the 7th Circuit Court of Appeals. I tried to explain to somebody who asked me about that -- not in a hearing, but a private citizen.

I said, "It happens. And it's not an indictment of the good faith of the prosecutor, of the district judge who denied a motion for a directed verdict or the jury that convicted. Sometimes appeals courts disagree about the inferences to be drawn from the evidence and reverse a conviction. That doesn't tell you that the prosecutor is a bad guy. In fact, I know this one, and this is a good guy."

KOHL: Mr. Comey, yesterday's Washington Post reported that White House and Republican Party concerns regarding voter fraud prosecutions were the cause of many of the U.S. attorney dismissals. Can you confirm this?

During the time you served as deputy attorney general were you aware of concerns from the White House that U.S. attorneys were not active enough in prosecuting voter fraud cases? Did the White House exert any effort to encourage the Justice Department to remove U.S. attorneys whom it believed were not prosecuting voter fraud cases vigorously enough?

COMEY: I'm not aware of any issue that came to my attention regarding voter fraud when I was deputy attorney general, complaints or otherwise.

KOHL: While you served at the Justice Department, were you aware of any pressure from the White House to bring voter fraud cases?

COMEY: No, sir.

KOHL: Thank you so much.

COMEY: Thank you, Senator.

KOHL: Mr. Chairman, thank you.

SCHUMER: Senator Feingold?

FEINGOLD: Mr. Chairman, first, I want to praise you for your questioning. It was very long. I hope you don't make it a habit.

But I'll tell you something: I think it was some of the most important and valuable questioning that I've heard from a senator in the years that I've been here. And I just want to thank you for your leadership on this.

Mr. Comey, I want to commend you for your service, for your courage, for your testimony, some of the most dramatic testimony that I've heard in 25 years that I've been a legislator. Your courage at the time and today in defense of the rule of law is truly admirable.

Let me add, your account of Attorney General Ashcroft is the same.

FEINGOLD: This has been my experience with Mr. Ashcroft, despite our fundamental differences.

And I have great disagreement with this administration. But there's a difference in this administration between people like you and Attorney General Ashcroft, who do fundamentally respect the rule of law, and many others who have shown some of the most blatant disrespect for the rule of law I think in American history.

So I think it's only fair that we make these distinctions. And I know that's not your purpose in being here. But I simply want it noted in the record that here's somebody that literally stood tall for the rule of law. And I praise you for it.

I want to highlight one point you alluded to in answer to a question from Senator Specter.

This reauthorization process and the need for certification from the attorney general was only an internal control, not a statutory requirement. I think that that testimony makes it all the more clear that this committee must pursue this issue, and must be supplied with the relevant documents.

So, Mr. Comey, are you aware of any documents produced by the White House Counsel's Office with regard to this program?

COMEY: Not specifically. Yes, not specifically. I don't remember...

FEINGOLD: You don't recall reviewing any...

COMEY: I don't remember reviewing any from the White House Counsel's Office that related to this. I mean, it's possible. But I don't remember it.

FEINGOLD: What about documents from the Office of the Vice President? Do you know if any such documents exist regarding this program?

COMEY: I don't, no.

FEINGOLD: Did Mr. Gonzales or Mr. Card indicate -- ever indicate that they were acting on the direction or the knowledge of the president when they came to see the attorney general in the hospital?

COMEY: Not that I recall. I don't think so.

FEINGOLD: They never stated that, to your recollection.

COMEY: I don't think so.

FEINGOLD: Did something in particular occur that led to this issue coming to a head in March of 2004? Why not at an earlier point, in connection to one of the earlier reauthorizations?

COMEY: It was simply the pace at which the work went on in the Office of Legal Counsel.

We had a new assistant attorney general as of, I think, October of 2003. And there were a number of issues that he was looking at. And this reevaluation, this particular program was among those issues. And the work got done in the beginning part of 2004. And that's what brought it to a head with this particular...

FEINGOLD: So it was at this point that the office was able to get around to these concerns, these legal concerns and these internal concerns?

COMEY: I think that's right.

Concerns had reached the ears of the new assistant attorney general. And he undertook an examination -- with my approval and Attorney General Ashcroft's approval -- of this matter.

FEINGOLD: You made quite a moving farewell address to your colleagues in the department in August of 2005. In it, you thanked some of your colleagues for being, quote, "people committed to getting it right and to doing the right thing, whatever the price," unquote, and stated that some of those people, quote, "did pay a price for their commitment to right," unquote.

What were you referring to?

COMEY: I had in mind one particular senior staffer of mine who had been in the hospital room with me and had been blocked from promotion, I believed, as a result of this particular matter.

FEINGOLD: And so you were, in fact, referring to this incident in the hospital and somebody who was there and consequences that accrued to this person as a result of that?

COMEY: Yes.

FEINGOLD: Is that Mr. Goldsmith?

COMEY: No, it's Mr. Philbin.

FEINGOLD: Thank you, Mr. Chairman.

SCHUMER: Senator Specter wants to make a concluding statement or...

SPECTER: Well, I just wanted to confirm with you, Mr. Chairman, that we're not going to have a second round.

SCHUMER: We're not going to have -- I have one question, which I've showed you, and that's it.

SPECTER: There's a vote scheduled in five minutes, so I'm going to go to the floor at this point.

And I conclude by thanking you for your service, Mr. Comey. And I thank you for standing up. That's in the finest tradition of the Department of Justice and I hope we can reinstate it. Thank you.

COMEY: Thank you, Senator.

SCHUMER: Well said.

Senator Whitehouse?

WHITEHOUSE: Thank the chairman.

Mr. Comey, good morning. It's still morning.

I'd like to ask you -- you are obviously a person who cares very deeply about the Department of Justice and its institutions. And I worry about some of the institutional legacy of what we've been through.

In particular, I'd like to ask you for your thoughts on where the standards should be of what is proper versus what is improper in the context of bringing political influence or partisan influence into the Department of Justice. And while you -- that's, sort of, the framing part of the question.

More specifically, I've been very concerned at some of the statements that have come out of the Department of Justice that have been the department's efforts to define that level of impropriety.

And I'll tell you, it began first with Kyle Sampson who told this committee that, "The limited category of improper reasons for these dismissals would include an effort to interfere with or influence the investigation or prosecution of a particular case for political or partisan advantage."

And then, not too much later, Attorney General Gonzales came before us, and in nearly verbatim words, he said that, "It would be improper to ask for a resignation of any individual in order to interfere with or influence a particular prosecution for partisan political gain."

And in the wake of the attorney general's testimony in the House, the Justice Department issued a statement saying that, "It is clear that the attorney general" -- again, defining the standard of what's improper -- "did not ask for the resignation of any individual in order to interfere with or influence a particular prosecution for partisan political gain."

WHITEHOUSE: Now, when I read those things I hearken back to the elements of obstruction of justice, which I recall as being three. One is the awareness of a particular case. Two is the effort to influence or interfere with it. And three is that that be done for a corrupt or improper motive, such as partisan political gain.

Let me ask it to you two ways.

The first way would be, if it became clear to you that somebody in the department had tried to interfere with or influence a particular prosecution for partisan political gain, would you consider that to be the basis for opening -- at least opening an obstruction of justice investigation?

And if the facts were proven, would that not even be the basis for a conviction for criminal obstruction of justice?

COMEY: I think it potentially could be, yes -- certainly for looking at the matter.

WHITEHOUSE: Yes.

And in that context, do you think that is where the bar should be set for what is improper versus not improper in terms of political influence coming into the Department of Justice? Is that the right standard?

COMEY: No. If the standard is whether we're running afoul of the obstruction of justice statute, I think it's set way too low.

Senator, as you know...

WHITEHOUSE: What should be? You've had the chance to think about this. You care about this department deeply. You've shown through what is probably a difficult experience for you that you're willing to think about these things without bias and really try to get to the right answer.

How would you phrase where the standard for what is improper should be in terms of where and when the department should allow political influence to enter into its deliberations or its conduct?

COMEY: I think that you have to talk about it in two pieces. One is main Justice and the other is the U.S. attorneys.

And although both of those parts of the institution are led by political appointees, I think they are -- have to be different in terms of what political means.

I think it is the job of the Department of Justice to be responsive to the policy priorities of the president, who's elected and who has appointed the folks to run the department.

COMEY: But I think it is main Justice's job to see to it that U.S. attorneys can operate in an environment where there is a little or no politics -- big P or little p -- at all entering into their considerations.

I think once they walk through the door and become the U.S. attorney, although they're politically appointed, they've got to call, as someone said, balls and strikes without regard to whether the person in the dock is a Democrat or a Republican or a Green or a who cares? They have to make the judgment the judgment on the facts.

I think the job of the department is, to the extent that there are complaints or their political issues, to receive those and figure out what to do about them without polluting the work of the U.S. attorney. And that's why I think they're different.

I think the hard thing to define in the abstract is certainly not obstruction of justice as the standard. I think the department needs to make its decisions about what to do with political interests or information by looking at what is the mission of the Department of Justice.

WHITEHOUSE: And do you agree with me that this standard that they've been articulating about efforts to interfere with or influence a particular prosecution for partisan political gain effectively restate the standard for a criminal obstruction of justice?

COMEY: It sounds like it does. And that's certainly something that should be avoided at all costs.

But I think it sets the bar a little too low in terms of what the department's mission is in protecting the historical autonomy of the entire department, especially the U.S. attorneys.

WHITEHOUSE: Mr. Chairman, my time has expired.

Thank you, Mr. Comey.

SCHUMER: Thank you, Senator Whitehouse.

Mr. Comey, I just want to follow up on one final question. I showed it to Senator Specter ahead of time because he had to leave.

But he was asking about legality/illegality, within law/not (ph). The key point here is isn't it the Office of Legal Counsel that makes a determination about whether something is within the law or not within the Justice Department?

COMEY: Yes. And its opinions are binding throughout the executive branch.

SCHUMER: And didn't that office make a decision and advise you that what was attempting to be done was not within the law?

COMEY: The conclusion was that they could not find an adequate legal basis for...

SCHUMER: OK. Let's put it that way.

COMEY: Yes.

SCHUMER: So they could not find an adequate legal basis for doing it that way?

COMEY: Correct.

SCHUMER: And you felt that if they couldn't, you couldn't preside over the Department of Justice if you were going to be overruled by the White House to do it anyway.

COMEY: Yes.

SCHUMER: I think that's OK.

Let me conclude, then, by just thanking you. You are a profile in courage. You are what our government is all about. In this case, it has nothing to do with Democrat, Republican, liberal, conservative. It has to do with doing a job well and caring about the rule of law.

And I would say what happened in that hospital room crystallized Mr. Gonzales' view about the rule of law: that he holds it in minimum low regard.

And it's hard for me to understand -- I'm going to say something that you won't say: It's hard to understand after hearing this story how Attorney General Gonzales could remain as attorney general, how any president, Democrat, Republican, liberal, conservative, could allow him to continue.

But I want to thank you for being here. I know it wasn't easy. I know that if we didn't have the power of subpoena you wouldn't be here. I know you have a conscience that obviously you've wrestled with in all this and it's very difficult to be here.

But a profile in courage, by definition, is difficult. And I think I speak on behalf of almost every American: We thank you for being here and having the courage to speak the truth.

(APPLAUSE)

END

May 15, 2007 12:34 ET
.

Written Questions to
Former Deputy Attorney General James B. Comey
Submitted by Senator Patrick Leahy
May 22, 2007

1. You testified that the Department of Justice ("DoJ") completed a factual and legal evaluation of "a particular classified program" in 2004, and this review was conducted by, among others, the Office of Legal Counsel ("OLC").

a. When was this review started?

I believe some time in late fall 2003.

b. Why was the review started? Was the review started at the request of any individual or entity? If so, who or what entity**?**

I believe it was started at the initiative of Jack Goldsmith and Patrick Philbin.

c. Who participated in the review? Other than OLC, did any other division, section, or unit at DoJ participate in the review?

Goldsmith and Philbin were the principal participants, as I recall. I believe they were assisted from time to time by James Baker from the Office of Intelligence Policy and Review and my chief of staff, Chuck Rosenberg. There may have been other DOJ lawyers who assisted them.

d. Did any individual or entity from outside DoJ participate in the review? Were there any individuals from the White House, the Department of Defense ("DoD"), or other federal agency who participated in the review? If so please identify those individuals and/or entities?

I believe Goldsmith and Philbin coordinated their effort with lawyers in the intelligence community.

e. Did the review assess the full duration of the classified program and, if not, what time frame was reviewed?

The review focused on current operations during late 2003 and early 2004, and the legal basis for the program.

f. As a result of the review, did any individual or entity at DoJ, or any other agency, prepare a legal opinion or memorandum related to the classified program, and, if so, who or what entity prepared the legal opinion or memorandum?

OLC prepared legal memoranda concerning the matter, some of which would have been drafts. I also prepared at least one memorandum.

g. Were the results of this review shared with the Federal Bureau of Investigation ("FBI"), and, if so, who at the FBI and when?

It is my understanding that Goldsmith and Philbin discussed their work with officials from the General Counsel's office at the FBI, including the General Counsel, Valerie Caproni. I discussed the matter privately with FBI Director Mueller and FBI Deputy Director John Pistole.

h. Other than the White House or individuals at the White House, were the results of this review shared with any individual, entity, or federal agency outside DoJ, and, if so, who or what entity and when?

The matter was discussed with lawyers and non-lawyers in the intelligence community. I am uncomfortable going into more detail in an unclassified setting.

2. In your testimony, you stated that the views of DoJ related to the classified program were communicated to the White House prior to the evening of March 10, 2004.

a. How were these views communicated to the White House? Please identify whether the communications were made orally, in writing, by electronic communication, or other means; and to whom and when the communications were made. Please identify if any of the documents responsive to Question 1 above were included in this communication.

The views were communicated orally prior to March 10, 2004, including at a March 9 meeting I attended at the White House. I also believe that Goldsmith and Philbin had a variety of contacts with officials at the White House in the preceding weeks or months as the review was conducted. Those contacts may have involved their sharing written materials, but I am not sure. I recall sending one memorandum to the White House, after March 10, which I believe attached a memorandum written by Goldsmith.

b. Without disclosing the substance of the classified program or any legal advice, did these views include the understanding that the Attorney General, or you as Acting Attorney General, would not certify the classified program?

Yes.

c. Did you or others at DoJ receive any response to these views from the White House? If so, please identify whether the responses were made orally, in writing, by electronic communication, or other means; and to whom and when was the response was made.

I directly received oral responses during discussions at the White House on March 9, 2004. I know there were a variety of discussions in early 2004 in which I did not participate but that involved Jack Goldsmith and Patrick Philbin.

d. Did the response include any legal opinion or memorandum from the White House, or any other federal agency related to the classified program? If so, please identify what individual(s) or entities prepared and reviewed the legal opinion or memorandum.

I am not aware of any other such memorandum or legal opinion prior to March 10, 2004. Some time shortly after March 10, I received a memorandum from White House Counsel Gonzales.

3. You testified that after you arrived at the George Washington Hospital in Washington, D.C., on the evening of March 10, 2004, White House Counsel Alberto Gonzales and White House Chief of Staff Andrew Card came to Attorney General John Ashcroft's hospital room and spoke to him relating to the authorization of a classified program.

a. Did any individual(s) come with Mr. Gonzales or Mr. Card to the hospital, and if so, who? Were those individuals present for the conversation between Mr. Ashcroft and Mr. Gonzales?

I do not know with whom Mr. Gonzales and Mr. Card arrived; only the two of them entered the room.

b. Upon arriving in the hospital room, did Mr. Gonzales say anything to you, either before or after his conversation with Mr. Ashcroft, and if so, what did he say?

He did not speak to me at any time.

c. Did Mr. Card speak to Mr. Ashcroft or you in the hospital room and if so, what did he say?

Mr. Card did not speak to me. I believe he said, "Be well," to Attorney General Ashcroft as he turned to depart.

d. To your knowledge, did Mr. Gonzales or Mr. Card consult with Mr. Ashcroft's physician or any medical staff prior to entering the hospital room?

Not to my knowledge.

e. In your presence, did Mr. Gonzales or Mr. Card ask Mr. Ashcroft questions to elicit his state of mind and/or medical condition prior to discussing their request for authorization of the classified program?

I believe Mr. Gonzales began the conversation by asking, "How are you General?" to which the Attorney General replied, "Not well."

f. To your knowledge, did Mr. Gonzales or Mr. Card take any steps to ensure that facts related to the classified program were not disclosed to individuals without proper clearances or an actual need to know who were present in the hospital room?

Not to my knowledge.

4. In your testimony, you stated that FBI Director Robert Mueller also arrived at the George Washington Hospital that night.

a. To your knowledge, did Mr. Mueller have any conversation with Mr. Gonzales or Mr. Card at the hospital that night? If so, what was that conversation?

Not to my knowledge.

b. In your testimony, you indicated that Mr. Mueller had a "memorable" exchange with Mr. Ashcroft after Mr. Gonzales and Mr. Card left. Please describe that exchange.

It was a private conversation in which Mr. Mueller expressed his admiration for the Attorney General's conduct that evening.

5. You testified that the President met with you privately, and then, at your urging, he also met with Mr. Mueller privately, on the morning of March 12, 2004 following your daily counter-terrorism briefing. After these discussions, you stated that the President indicated to Mr. Mueller that you were now authorized to make changes to the classified program in response to the Department of Justice's views.

a. Following your meetings, did the President direct you or Mr. Mueller to discontinue or suspend any portion of classified program immediately until the appropriate changes were made to bring it into legal compliance?

No.

b. How long did the classified program continue without legal certification from DoJ?

I don't recall exactly, but believe it was approximately several weeks.

6. You testified that you discussed DoJ's views on the classified program with Vice President Dick Chaney and members of his staff, including his Chief of Staff David Addington.

a. Where and when did those discussions take place?

March 9, 2004 at the White House.

b. Who else was present for those discussions?

Jack Goldsmith, Patrick Philbin, Vice President Cheney, Mr. Addington, Mr. Card, Mr. Gonzales, and members of the intelligence community.

c. If those discussions were on or before March 10, 2004, was the Vice President and/or his staff aware of DoJ's decision not to certify the classified program? If so, how were they aware?

Yes. The Vice President was aware of DOJ's decision to not certify the program, because I had communicated this orally during a March 9 meeting. That meeting was a culmination of ongoing dialogue between DOJ and the White House.

d. If those discussions were on or before March 10, 2004, was the Vice President and/or his staff aware of your intention to resign if the classified program was authorized without DoJ certification? If so, how were they aware?

No. I had not made a decision to resign yet.

e. To your knowledge, did the Vice President or his staff have any role in the decision to have Mr. Card and Mr. Gonzales visit Mr. Ashcroft in the hospital? If so, what role did they have and what is the source for your information?

I have no knowledge about that.

7. You testified that Mr. Philbin, who was with you in the hospital, was "blocked from promotion," as a result of the position taken by DoJ related to this classified program.

   a. Did any individual or individuals from the White House have any input into his potential promotion at DoJ? If so who, and in relation to what promotion?

   Mr. Philbin was considered for principal Deputy Solicitor General after Paul Clement became Solicitor General. It was my understanding that the Vice President's office blocked that appointment.

   b. Who was involved in blocking Mr. Philbin's promotion, and what did they do?

   I understood that someone at the White House communicated to Attorney General Gonzales that the Vice President would oppose the appointment if the Attorney General pursued the matter. The Attorney General chose not to pursue it.

8. When did the Administration first conclude that the Authorization for Use of Military Force ("AUMF") authorized warrantless electronic surveillance of the type involved in what the Administration has called the "terrorism surveillance program" or TSP? If you do not recall a specific date, please provide as close an approximation as is possible.

   I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

9. What legal standard for intercepting communications was the National Security Agency ("NSA") applying in its warrentless electronic surveillance program before March 2004? Was it a "probably cause" standard? What standard was the NSA applying when the program was first authorized? What standard was applied after March 2004?

   I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

10. Has the warrantless electronic surveillance program always required before authorizing interception of a communication that at least one party to the communication be located outside of the United States? If not, approximately when did this become a requirement?

    I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

11. Has the warrantless electronic surveillance program always required before authorizing interception of a communication that at least one party to the communication be a member or agent of Al Queda or an affiliate terrorist organization? If not, approximately when did this become a requirement?

    I don't think it is appropriate for me to discuss legal advice by the Department of Justice or any particular classified program.

Written Questions from Senator Charles E. Schumer to James B. Comey
May 15, 2007 Hearing

1. When the Attorney General testified before the Senate Judiciary Committee on February 6, 2006, he stated that there was little or no dissent within the Administration with respect to the program that "the President has confirmed."

   - **Was the classified program over which you and others almost resigned in March 2004 the program that the President confirmed in early 2006? Was it a variant of the program the President confirmed in early 2006?**

I do not believe I can answer these questions in an unclassified environment.

2. You testified that in March of 2004, while Attorney General Ashcroft was hospitalized with pancreatitis, the powers of the Attorney General were transferred to you.

   - **Please describe the mechanism by which that power was transferred to you, what documentation was created, what public statements were made about the transfer, and what communications were had with White House personnel about the transfer.**

David Ayres, the Attorney General's Chief of Staff, handled the documentation and notifications to the White House. He would have worked with my Chief of Staff, Chuck Rosenberg. I do not recall what specific documents were created. There was media coverage about the fact that I was acting Attorney General and I believe DOJ Public Affairs made public statements to that effect.

3. Please identify all the officials at the Department of Justice or elsewhere whom you have a basis to believe were prepared to resign in March 2004 over the classified program you alluded to in your testimony.

I believe the following individuals were prepared to resign: Jack Goldsmith, Patrick Philbin, Chuck Rosenberg, Daniel Levin, James Baker, David Ayres, David Israelite, Robert Mueller. Although not involved with the matter, I believe a large portion of my staff would have resigned were I to depart.

4. You testified that you believed that your former aide, Patrick Philbin, had been blocked from promotion as a result of his participation in the dispute over the classified program you alluded to. Specifically, it has been reported in the press that Mr. Philbin was blocked from taking the position of Principal

Deputy Solicitor General because of the objections of Vice President Cheney and his aide, David Addington.

- **Can you confirm the accuracy of these media accounts? If they are inaccurate, please identify the particular promotion that was denied to Mr. Philbin, the individuals who objected, and the circumstances surrounding Mr. Philbin's being rejected for the promotion.**

I believe they are accurate.

5. You testified that during the visit to Attorney General Ashcroft's hospital room on the evening of March 10, 2004, Mrs. Ashcroft was present when you first arrived and also later when Messrs. Gonzales and Card arrived.

- **Did you reveal classified information in Mrs. Ashcroft's presence?**

No.

- **Did either Mr. Gonzales or Mr. Card reveal classified information in Mrs. Ashcroft's presence?**

Mr. Card did not. I do not recall whether Mr. Gonzales mentioned any aspects of the matter that would be considered classified, including the name of the program – which was itself classified, as I recall – when addressing Mr. Ashcroft.

6. You testified that in or about March 2004, the Justice Department's Office of Legal Counsel determined that it could not certify the legality of the classified program you alluded to in your testimony.

- **Did the Office of Legal Counsel or any other office prepare a written opinion providing the basis for concerns about the legality of the classified program you alluded to in your testimony? If so, please identify the approximate date(s) of any such opinion, the author(s), and the recipients of any such opinion, inside and outside the Justice Department.**

Yes. OLC prepared legal memoranda concerning the matter during early 2004, some of which would have been drafts. I also prepared at least one memorandum that I recall. The Department of Justice would be in the best position to supply dates and information about recipients.

7. As you may know, Todd Graves has recently said that he was asked to resign in January of 2006, making him at least the 9th United States Attorney who was dismissed last year.

- **Did you form an opinion of the quality of Mr. Graves's work when you were the Deputy Attorney General? If so, what was it?**

I had a positive impression of Mr. Graves and believed he was performing well as U.S. Attorney.

- **What was John Ashcroft's opinion of Mr. Graves, if you know?**

I believe Attorney General Ashcroft shared my opinion of Mr. Graves, although I do not recall a specific conversation with Mr. Ashcroft concerning Todd's performance.

8. I know that you are familiar with the highest-ranking career official at the Justice Department, David Margolis. He has testified that in November of 2006, Kyle Sampson read him a list of several names of U.S. Attorneys who would be asked to resign. In response, Mr. Margolis made clear that so long as people were being dismissed, there were two U.S. Attorneys who were very poor performers who deserved to be fired. One, he said, was Kevin Ryan, who by many accounts had management and other issues in the Northern District of California. The other U.S. Attorney, whom Mr. Margolis did not identify, was not dismissed and continues to serve as a U.S. Attorney today.

   - **What do you make of the fact that the same people who decided to fire Dan Bogden of Nevada for no apparent reason also refused to heed Mr. Margolis's advice with respect to this other U.S. Attorney?**

   I don't know what to make of it. Mr. Margolis is a wise person with significant experience in personnel matters, whose advice is always worthy of serious consideration.

9. You are the Department official who decided – after I called for it – to appoint a Special Prosecutor in the Valerie Plame affair. After John Ashcroft recused himself from the issue, you appointed your former colleague, Patrick Fitzgerald. And you performed the delegation of duties to Mr. Fitzgerald with respect to the Plame investigation.

   - **If Mr. Fitzgerald were fired as U.S. Attorney, would he have been able to continue as Special Prosecutor under your delegation of authority?**

I don't believe so because he was appointed in his capacity as United States Attorney.

10. You testified before the House a few weeks ago that you had a 15-minute conversation with Mr. Sampson on February 28, 2005 – shortly after Alberto

Gonzales took over as Attorney General. You testified that you discussed two things. One was a conversation about who you thought were the weakest U.S. Attorneys. You were never asked about the second topic.

- **What was the second subject? Please provide details of that portion of your conversation with Mr. Sampson.**

This conversation occurred shortly after Attorney General Gonzales's confirmation. Mr. Sampson explained to me a vision for the operation of the Attorney General's office and the Office of the Deputy Attorney General that would involve operating those respective staffs as essentially one staff. My understanding was that this vision would entail the Deputy Attorney General and staff acting in much closer coordination with the Attorney General and his staff. I responded that I believed it was very valuable to the Attorney General and the Department for the Deputy Attorney General to act as a separate office and that I did not support this vision.

I thought such an arrangement risked elimination of the separate vetting and advice function of the DAG and his or her staff. There is great value in having that office – called ODAG -- available to make decisions that need not reach the Attorney General or to review and advise on matters headed to the Attorney General for decision. The risk inherent in combining the staffs is that the separate review and advice function is lost, which would not be in the interest of the Attorney General or the Department.

Questions for the Record for James Comey (Senator Feingold)

1. In testimony before the House and Senate Judiciary Committees in 2006, Attorney General Gonzales stated that that there were not any serious disagreements between you and others within the Administration relating to the NSA wiretapping program confirmed by the President. After your testimony last week, Senators Schumer, Kennedy, Durbin and I sent a letter to the Attorney General asking if he wished to revise that testimony. The Attorney General responded that his testimony was accurate. (See attached letter and response.)

a. Based on your knowledge of what transpired within the Administration when you were Deputy Attorney General, do you agree with the Attorney General that his testimony in 2006 "was and remains accurate"?

I do not believe I can answer that question in an unclassified environment.

b. Was his testimony misleading?

I do not believe I can answer that question in an unclassified environment.

2. The Attorney General has stated repeatedly that although he did not personally look into the rationales behind why each attorney should be fired, he approved the list of U.S. Attorneys to be fired because he believed the list reflected a consensus judgment of the "senior leadership of the department." For example, on Thursday, April 19, 2007, he testified:

> "What I understood was that the recommendations reflected the consensus judgment of the senior leadership of the department and that, therefore, the senior leadership had lost confidence in these individuals and thus the department had lost confidence. . . I understood that the senior leadership, that the recommendation made to me reflected the consensus view of the senior leadership of the department, of individuals who would know better than I about the qualifications of these individuals."

This testimony suggests that there was a serious and deliberative process that yielded these judgments, yet virtually every senior DOJ official who has testified in our investigation has disavowed any significant or active involvement in selecting which individuals should be fired. For example, Mr. Sampson, the Attorney General's former chief of staff, suggested that you played a role in selecting the attorneys for firing, but you testified to the House on May 3, 2007, that you were "not aware that there was any kind of process going on or that my very brief conversation with Mr. Sampson was part of some process to figure out a group of U.S. attorneys to fire."

Deputy Attorney General Paul McNulty, Principal Associate Deputy Attorney General William Moschella, Associate Deputy Attorney General David Margolis, Acting Associate Attorney General William Mercer, Former Director of the Executive Office of U.S. Attorneys Michael Battle, the Chief of Staff to Mr. McNulty, Michael Elston, and Counselor to the Attorney General Matt Friedrich have all reported little to no involvement in personally recommending individual attorneys for this list. Mr. Sampson has characterized his function as merely aggregating the recommendations of others and then passing those recommendations on to the Attorney General and has denied that any of the individuals were on the list because he personally wanted them there.

a. If this had actually been a legitimate and serious process, who would have been consulted for their opinions on this matter? Which positions at DOJ are held by people who you think can speak with authority on the performance of specific U.S. Attorneys?

An evaluation of the performance of U.S. Attorneys should involve, at a minimum, the Deputy Attorney General and members of his staff who interacted with the U.S. Attorneys and officials at the Executive Office for U.S. Attorneys who deal regularly with, and inspect, the U.S. Attorneys.

b. If this had actually been a legitimate and serious process, what records would you expect would have been created for the Attorney General and the Deputy Attorney General to document it?

I have never been involved in such a review process so I do not know what types of documents would be created. In my opinion, the EARS evaluations should be a critical part of any review process, either for an individual U.S. Attorney or for a broader group review.

c. Other than the officials mentioned above, can you think of any other "senior Department officials" who the Committee should ask if they were involved in determining which U.S. Attorneys should be fired?

No.

d. If, in fact, the senior leadership of the department was not involved in generating the names of individuals to be fired, who should the Committee look to in order to understand why the specific fired U.S. Attorneys—other than Mr. Ryan from San Francisco—were singled out?

I do not know.

3. You testified in the House that Kyle Sampson met with you for about 15 minutes on February 28, 2005, and asked you who the weakest U.S. Attorneys were. You gave him several names. You testified that of those names, only Kevin Ryan ended up on the list to be fired. You did not mention any of the other fired U.S. Attorneys and in fact, you testified that you had and have quite favorable opinions of many of them. Just two days after your meeting with him, on March 2, Mr. Sampson sent a preliminary chart reflecting his assessment of all 93 U.S. Attorneys to Harriet Miers in the White House. That list shows Kevin Ryan as a strong U.S. Attorney and lists Margaret Chiara, Bud Cummins, and Carol Lam as U.S. Attorneys to consider removing.

a. If this were a legitimate and serious process, where senior officials of the Department were being consulted, and Mr. Sampson had received information suggesting that Chiara, Cummins, and Lam should be removed for legitimate reasons, would you have expected him to have specifically asked your opinion about these U.S. Attorneys when he met with you two days before?

Yes.

b. If the information Mr. Sampson obtained about Kevin Ryan was so different than your assessment, shouldn't he have discussed that with you as well?

Yes.

4. In an unfortunately prescient section of your farewell address to Department of Justice employees on August 2005, you discussed the fact that the good work that DOJ accomplishes is made possible by "a reservoir of trust and credibility" that the public has for the Department. You also noted that "the problem with reservoirs is that it takes tremendous time and effort to fill them, but one hole in a dam can drain them. The protection of that reservoir requires vigilance, an unerring commitment to truth, and a recognition that the actions of one may affect the priceless gift that benefits all."

a. Is the matter of the fired U.S. Attorneys an example of such a hole in that dam, one that affects the trust and credibility of the Department and has implications far beyond the lives and reputations of the individual U.S. Attorneys?

Yes. The entire affair has harmed the Department and its reputation.

b. What should be done, in your view, to repair the credibility of the Department and the American people's trust in it? In particular, what steps should be taken internally by the Department of Justice or by the Administration as a whole?

Time and distance, and the everyday good work of the Department's thousands of trustworthy and honest people all over the country, will help to repair the harm. We should remember that this is a Department that survived – and even thrived – following the Watergate era. As painful as this time is, the great and positive institutional inertia of the organization – composed of people who love doing good for a living – will be its salvation.

c. Are there things that we in Congress should do either to help restore DOJ's reputation or to prevent this sort of thing from happening in the future?

It would be a good thing if Congress shone a light on the good work being done by the men and women of the Department all over the country. There is much good out there that gets too little attention.

Exhibit 2

FEDERAL BUREAU OF INVESTIGATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JULY 26, 2007

Serial No. 110–86

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

37–010 PDF WASHINGTON : 2007

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

JOHN CONYERS, Jr., Michigan, *Chairman*

HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
LINDA T. SÁNCHEZ, California
STEVE COHEN, Tennessee
HANK JOHNSON, Georgia
BETTY SUTTON, Ohio
LUIS V. GUTIERREZ, Illinois
BRAD SHERMAN, California
TAMMY BALDWIN, Wisconsin
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
ARTUR DAVIS, Alabama
DEBBIE WASSERMAN SCHULTZ, Florida
KEITH ELLISON, Minnesota

LAMAR SMITH, Texas
F. JAMES SENSENBRENNER, Jr., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
CHRIS CANNON, Utah
RIC KELLER, Florida
DARRELL ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio

Perry Apelbaum, *Staff Director and Chief Counsel*
Joseph Gibson, *Minority Chief Counsel*

CONTENTS

JULY 26, 2007

Page

OPENING STATEMENTS

The Honorable John Conyers, Jr., a Representative in Congress from the State of Michigan, and Chairman, Committee on the Judiciary 1
The Honorable Lamar Smith, a Representative in Congress from the State of Texas, and Ranking Member, Committee on the Judiciary 2

WITNESSES

The Honorable Robert S. Mueller, III, Director, Federal Bureau of Investigation
Oral Testimony 3
Prepared Statement 7

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Prepared Statement of the Honorable Sheila Jackson Lee, a Representative in Congress from the State of Texas, and Member, Committee on the Judiciary 62
Prepared Statement of the Honorable Betty Sutton, a Representative in Congress from the State of Ohio, and Member, Committee on the Judiciary 73
Post-Hearing Questions posed by the Honorable John Conyers, Jr., and the Honorable Luis V. Guiterrez to the Honorable Robert S. Mueller, III, Director, Federal Bureau of Investigation 74
Letter from Richard C. Powers, Assistant Director, Office of Congressional Affairs, U.S. Department of Justice, Federal Bureau of Investigation, dated November 13, 2007 84
Letter from Richard C. Powers, Assistant Director, Office of Congressional Affairs, U.S. Department of Justice, Federal Bureau of Investigation, dated December 19, 2007 85

I am not certain about our intersection with the group at the University of North Texas, and I would have to get back to you on that. Quite clearly, the developments we have had in DNA over the last number of years have transformed in some sense the criminal justice system—giving us positive identifications of individuals, whether it be persons who were subsequently successfully prosecuted, but also missing persons.

As the use of DNA grows, we are short of resources, we are backlogged. And whether it be for the missing persons database or to more effectively and efficiently process requests for DNA examinations, it is something where we are going to need substantial resources in the future. My belief is the Federal system we have that integrates the State systems is working overall very well.

Mr. CHABOT. Thank you very much.

I think my time has expired, Mr. Chairman. Thank you.

Mr. CONYERS. Thank you.

I would be pleased to recognize the indefatigable gentlelady from Houston, Texas, Sheila Jackson Lee.

Ms. JACKSON LEE. Welcome to Mr. Mueller.

Thank you very much, Mr. Chairman. Let me thank you for creating a very important—or expanding on the very important role of this Committee, and that is oversight.

And we welcome you, Mr. Mueller. I know that we have visited before and you have missed some times. We hope you are well. Thank you for that.

I have three questions. My time is very, very short. And I think in the spirit of oversight, we have some very, very important questions to focus on that address a line of questioning that we have addressed over the past couple of weeks.

It is March 10 when General Ashcroft was in the hospital and you got a call from Jim Comey, concerned about a meeting that Mr. Gonzales was going to have with the chief of staff of the White House.

And it seems as if you would dispatch your FBI detail so that Mr. Comey would not be evicted from the room with General Ashcroft. And I might say that all of us were wishing him well at that time—certainly expressed our concern.

But he was going there, General Gonzales, to talk about the TSP, warrantless wiretapping. And it is a concern, so that we can get the record straight about what happened. And Mr. Comey was—as he arrived, he expressed a number of concerns about what this meeting was going to be about.

So my question to you, first of all, did you ever speak with either Mr. Gonzales or Mr. Card while they were at the hospital?

Mr. MUELLER. No, ma'am.

Ms. JACKSON LEE. And if you did not do that, did any of your agents speak to those individuals?

Mr. MUELLER. I don't believe so. I arrived at the hospital after Mr. Gonzales and Mr. Card had left.

Ms. JACKSON LEE. The discussion—and I don't know if you did arrive—did you have an opportunity to talk to General Ashcroft or did he discuss what was discussed in the meeting with Attorney General Gonzales and the chief of staff?

Mr. MUELLER. I did have a brief discussion with Attorney General Ashcroft.

Ms. JACKSON LEE. Pardon? I am sorry?

Mr. MUELLER. I did have a brief discussion with Attorney General Ashcroft after I arrived.

Ms. JACKSON LEE. And did he indicate the details of the conversation?

Mr. MUELLER. I prefer not to get into conversations that I had with the Attorney General. At the time I—again, he was entitled to expect that our conversations——

Ms. JACKSON LEE. And I respect that. Could I just say, did you have an understanding that the discussion was on TSP?

Mr. MUELLER. I had an understanding the discussion was on an NSA program, yes.

Ms. JACKSON LEE. I guess we use TSP; we use warrantless wiretapping. So would I be comfortable in saying that those were the items that were part of the discussion?

Mr. MUELLER. The discussion was on a national—an NSA program that has been much discussed, yes.

Ms. JACKSON LEE. Well, I appreciate that.

And do you then later remember what might have occurred? We know that there was a meeting back at the White House that night. Again, all of us were interested. It was raising debate in the United States Congress. Do you remember what happened at the meeting at the White House that night?

Mr. MUELLER. I was not present at the White House that night.

Ms. JACKSON LEE. And would you have any recollection, or asked for recollection through staff, whether TSP was discussed?

Mr. MUELLER. Well, I was not present at the meeting that Mr. Comey testified to having later that night at the White House. I do believe it related to a national security program—or a national NSA program, I should say.

Ms. JACKSON LEE. And let me just be clear, because I am saying this to you. Is it your understanding that General Gonzales was at the hospital and visited then-former General Ashcroft along with the chief of staff, Andy Card? Is it your understanding that they did have a meeting?

Mr. MUELLER. Yes.

Ms. JACKSON LEE. And so as we listen to General Gonzales's testimony, I believe under oath, regarding that, his statement, if I might just indicate that, in a question posed to him—and if it was about the TSP you are dissembling to this Committee—now, was it about TSP or not, the discussion on the 10th?

I think this says the 8th; I think the transcript is incorrect. This was a question posed by Senator Schumer.

The answer was, the disagreement on the 10th was "about other intelligence activities." The question, specifically, was, was it about TSP or not? And the answer was "about other intelligence activities."

It appears, from our discussion here today, that the discussion was certainly more focused than what General Gonzales has offered to the United States—in your recollection?

Mr. MUELLER. I am sorry. Is that a question, ma'am?

Ms. JACKSON LEE. Yes, it is.

Mr. MUELLER. I really can't comment on what Judge Gonzales was thinking or saying. I can tell you what I understood at the time.

Ms. JACKSON LEE. I think we appreciate your recollection. And I will just follow up—just to finish, Mr. Chairman, if I may—to say that, General, I had a series of questions about hate crimes and about that watch list.

I would only say to you, on the watch list, there are many people hurting, as my colleague said, while others may be going free.

I would like to get a report back on the watch list, because I will speak for the Texas Medical Center. And researchers and scientists are on that list—and it is very destructive—among others.

My last point is, Mr. Chairman, is that we like your priorities on terrorism, but, if I may just show this, we have no action on hate crimes and racial violence. That is where you are in the investigation of those.

And so I would appreciate a quick answer or a letter back on why we are so low. And I would welcome the letter, if the Chairman does not indulge me at this point.

Mr. MUELLER. Well, if I may comment on that last point, the addressing of hate crimes, the addressing of civil rights abuse is our number-two priority. But I would look at that figure in terms of what it represents in actual investigations we have undertaken.

Because, for a substantial period of time, we would open cases to report that which has happened in a particular community, as opposed to a thorough investigation.

And I will absolutely get back to you. But I do not believe that those statistics reflect what we have done in terms of hate crimes of civil rights abuses.

Ms. JACKSON LEE. I thank you very much.

Mr. Chairman, I want to pursue in the Committee——

Mr. CONYERS. The gentlelady's time——

Ms. JACKSON LEE [continuing]. The conflicting testimony of General Gonzales.

Mr. CONYERS [continuing]. Has expired.

Ms. JACKSON LEE. Thank you very much. I yield back.

Mr. CONYERS. I would like to recommend that there will be questions coming to the Director from Members, that he will be able to respond to.

I am pleased now to recognize Dan Lungren, the distinguished gentleman from California.

Mr. LUNGREN. Thank you very much, Mr. Chairman.

Mr. Mueller, let me try and go back to the FISA warrants, versus the NSLs, just so we make sure that the record is correct. Because you said you can get more in FISA warrants than you can get in NSL, leading to the suggestion that you don't need NSLs because you have FISA warrants.

But as I understand your testimony, you use the NSLs in some ways in preparation to be able to get a FISA warrant, because the NSLs gives you non-content material. And you may not have the basis to go after the more extensive information, absent that which you would get through the NSL.

Is that correct?

Mr. MUELLER. Correct.

We have a task force, MS-13 task force, with a number of participants from various agencies that address this across not only the different State borders within the United States but transnationally. Approximately a year ago, there were some 600 MS-13 individuals who were arrested not only in the United States, but in El Salvador and Guatemala, Mexico, I think it may have been Dominican Republic, Honduras in a coordinated takedown.

With a gang such as this that crosses borders, it is a function of globalization, a different type of globalization which requires us to work cooperatively and build allegiances and alliances with our counterparts overseas, if we are to effectively address what I would call a scourge of gang activity.

As I mentioned—I would finish by saying that we have been somewhat successful recently in a joint task force operating out of Los Angeles to address violent crime with MS-13 and the 18 street gangs there.

Mr. FORBES. And if I could follow up on that—and I know you did have that success. You mentioned it earlier. How important are the joint task force capabilities to be able to pull down the gang networks that you are seeing, especially the national connectivity that we are beginning to see with MS-13?

Mr. MUELLER. My belief is task forces are tremendously important. And that it is tremendously important that State and local law enforcement authorities be funded to support task forces.

The funding constraints on State and local law enforcement have been somewhat substantial over the last years. We ask them to participate in joint terrorism task forces, to join with us in addressing the threat of terrorism. They ask us to participate with them to address what is most on their mind, which often is violent crime and, quite often, violent crime at the hands of gangs.

And the funding for both us, as well as State and local law enforcement, to address this must be provided, if we are to make a dent in violent crime activity, violent gang activity in the United States.

Mr. FORBES. And the last question—you may, if you don't have this statistic with you, just get back to us with it. Do you have any idea about the percentage of members of, let us say MS-13, because that is in the news lately, might be here illegally?

Mr. MUELLER. I do not. I would have to get back to you. But it is fairly—well, I would really have to get back to you on that. I don't want to——

Mr. FORBES. We have had testimony that it could be between 60 percent and 80 percent. But if you could just see what your statistics and get back.

Mr. MUELLER. Will do.

Mr. FORBES. Thank you, Mr. Director.

And, Mr. Chairman, I yield back.

Mr. CONYERS. Thank you very much, Mr. Forbes.

The Chair is pleased to recognize the gentleman from Tennessee, Mr. Steve Cohen.

Mr. COHEN. Thank you, Mr. Chairman.

I know we have gone over, two or three times, this fact that General Ashcroft was in the hospital. But I am curious. Mr. Comey said that he called you, and you called your agents and said that Mr. Comey was not to be removed from the room.

Why did you feel that there might be an attempt to remove him from the room?

Mr. MUELLER. It was based on my conversation with Mr. Comey, in which he indicated he had a concern that he would not be participating in discussions in which he felt he should be participating as the Acting Attorney General.

Mr. COHEN. And were there FBI agents at the room protecting General Ashcroft?

Mr. MUELLER. Yes. He had a detail of FBI agents throughout his tenure.

Mr. COHEN. All right. And so, he was concerned that Mr. Card and Mr. Gonzales, or Judge Gonzales, were not going to include him in the conversation. Is that correct?

Mr. MUELLER. All I can tell you is what I learned from him.

Mr. COHEN. So he believed that.

Mr. MUELLER. Yes.

Mr. COHEN. Why did you rush there?

Mr. MUELLER. He requested that I be there to determine what went on. You would have to ask Mr. Comey why he had me there. I did go at his request. He was the Attorney General at the time.

Mr. COHEN. So you went there, and when you were there, he said at one point that you had a brief and memorable conversation—a brief, memorable exchange with the Attorney General. How memorable was that?

Mr. MUELLER. I had a conversation with him. I couldn't recite to you word for word what that conversation was. I do remember him being there.

Mr. COHEN. Just a memorable conversation——

Mr. MUELLER. It was a conversation, yes.

Mr. COHEN. What was the gist of it, sir?

Mr. MUELLER. I guess it covered very generally what had happened the moments before.

Mr. COHEN. And what had happened the moments before?

Mr. MUELLER. Well, again, I resist getting into the conversations, the specifics of conversations I had, because I do think the Attorney General then, the Attorney General now, and others are entitled to keep those conversations between themselves.

Mr. COHEN. They may be entitled to, but are you entitled to?

And he is no longer the Attorney General, so at this point, he is not the Attorney General. I am asking you to tell us what the conversation was. I don't think there is a privilege.

Mr. MUELLER. Excuse me just 1 second.

Mr. COHEN. Sidebar.

Mr. MUELLER. The discussion was that there had been a prior discussion about an NSA program and that the Attorney General deferred to Mr. Comey as the person to make whatever decision was to be made.

Mr. COHEN. He had confidence in Mr. Comey, I take it.

Mr. MUELLER. Yes.

Mr. COHEN. Okay. At some point or another, I think you told maybe Mr. Watt that you felt that there were problems with some of the operations there, the wiretaps.

Mr. MUELLER. At a point in time, in conversations with Mr. Comey, I had understood that the Department of Justice had some concerns about the legality of an NSA program. That affected the FBI in the sense that we received pieces of information from the NSA.

My purpose was to determine that whatever we did as the Bureau in handling that was done according to the directive and the appropriate directive of the Department of Justice.

So my concern was to assure that whatever activity we undertook as a result of the information we received was done appropriately and legally. At some point in time, he expressed concern about the legality of it.

Mr. COHEN. And because of that concern, at some point did you express to Mr. Watt, I believe that was correct, earlier, that you considered resignation?

Mr. MUELLER. I don't believe I expressed that. I did not dispute what Mr. Comey had said. But, again, in this area, I would say that I should not get into the conversations I had with individuals.

Mr. COHEN. Well, this wouldn't be a conversation. I go back to Mr. Comey's testimony to the Senate—was about resignations. And Mr. Schumer asked, "Was one of those people that might have resigned the Director?" And he said, "I believe so. You would have to ask him, but I believe so."

So I am not asking you about a conversation with Mr. Comey, I am asking you, was he correct? Or better yet, just were you that person?

Mr. MUELLER. I was that person to whom he refers, yes.

Mr. COHEN. And were you considering resigning? You don't have to relay the conversation, this is just your own mind——

Mr. MUELLER. Understand why I cannot say that I do not dispute what Mr. Comey says, because Mr. Comey says ask Mr. Mueller. I will tell you that I don't believe that it is appropriate of me to get into conversations that I have had with principals on that issue.

Mr. COHEN. And I don't want a conversation. I want what is in your psyche. Did you consider it yourself? That is not a conversation, that is a state of mind.

Mr. MUELLER. Well, to the extent that I followed through on the state of mind, then it is a conversation. Again, I would resist getting into that conversation.

Mr. COHEN. My time is almost up. If I could have 30 more seconds, Mr. Chairman? And I would just like to ask this.

You made a comment about some task forces doing a great job in reducing crime in New York and Los Angeles. I am from Memphis. We have a serious crime problem there. Is there any plan to have any task forces there, street task forces, or additional personnel to help us with our crime problem?

Mr. MUELLER. I am quite confident we have at least one, if not more, safe streets task forces in Tennessee, in particularly in Memphis. And I will get back to you on that.

Mr. COHEN. No matter how many it is, I want one more. [Laughter.]

Mr. MUELLER. I would have to go look, but I do not believe that to be the case at all.

Mr. GOHMERT. All right, thank you.

And I do appreciate the Chairman's flexibility.

And, Mr. Mueller, I do thank you for coming up here and visiting with you. I think this helps us to have a better relationship. Thank you.

Mr. MUELLER. Thank you, sir.

Mr. CONYERS. The Chair recognizes yet another prosecutor, the gentleman from Alabama, Mr. Artur Davis.

Mr. DAVIS. Thank you, Chairman Conyers.

Mr. Mueller, I didn't know that my friend from Texas was going to be the first witness to beat you up today. That is news to those of us on this side.

Let me, in the time that I have, go back to something that we have obviously talked about a lot today, and it is the circumstances around the March 10 visit from the Attorney General to then-White House counsel Gonzales' office to Mr. Ashcroft, then the Attorney General.

And I will preface it by saying that I know you feel that we have plowed over this ground a lot today. We are doing it for an obvious reason. There have been serious questions raised about whether the current Attorney General was candid and truthful in his testimony at the United States Senate. And I know that you, if you had an opinion of that, would not venture it to us.

But it is important and we have some obligation to try to elucidate facts around as much as we can. So in that spirit, let me try to fill in some of gaps that some of my colleagues may have left today.

What did you understand John Ashcroft's condition to be on March 10, 2004?

Mr. MUELLER. He had gone through a difficult operation and was being closely monitored in the hospital.

Mr. DAVIS. Had you been in touch with him in the interim between March 10 and his operation?

Mr. MUELLER. No. The operation preceding March 10?

Mr. DAVIS. Yes, that is right. That is right.

Mr. MUELLER. No, I had not. I had not.

Mr. DAVIS. Did you understand him to be in a condition to receive visitors on these serious matters?

Mr. MUELLER. I did not, no.

Mr. DAVIS. Had you felt anything was pressing enough for you to get in touch with him during that timeframe?

Mr. MUELLER. No.

Mr. DAVIS. Were you surprised when you received the phone call from Mr. Comey indicating that there was going to be this visit to Mr. Ashcroft by Mr. Gonzales and Mr. Card?

Mr. MUELLER. It was out of the ordinary.

Mr. DAVIS. And was one of the reasons it was out of the ordinary because you didn't understand Mr. Ashcroft to be in a condition to receive visitors on serious matters?

Mr. MUELLER. No. It was a request from Mr. Comey that was out of the ordinary.

Mr. DAVIS. What was out of the ordinary?

Mr. MUELLER. To be requested to come to the hospital at that particular time, early in the evening.

Mr. DAVIS. And I think you have testified, or there has been testimony from Mr. Comey, that he asked you to have a conversation with FBI agents and to instruct them not to remove him from the room. Is that essentially accurate testimony on Mr. Comey's part?

Mr. MUELLER. I have no dispute with Mr. Comey as in that regard. My own recollection is somewhat uninformed.

Mr. DAVIS. Well, that certainly strikes me as unusual. You are the FBI Director. A senior official calls you and says, "Make sure that I am not evicted from the room," and I am sure that must have struck you as being an unusual request, didn't it?

Mr. MUELLER. Yes.

Mr. DAVIS. Did you take notes and memorialize your conversation with Mr. Comey, at that point?

Mr. MUELLER. No, at that point, I did not.

Mr. DAVIS. At some point, did you memorialize your conversations regarding this visit with Mr. Comey?

Mr. MUELLER. I may have, yes.

Mr. DAVIS. Do you still have those notes?

Mr. MUELLER. Yes.

Mr. DAVIS. And are they available to the Committee if the Committee was to ask for them?

Mr. MUELLER. I would have to get back to you on that.

Mr. DAVIS. Can you think of a reason or a privilege that would prevent the Committee from receiving these notes?

Mr. MUELLER. Deliberative, but I would have to get back to you on that.

Mr. DAVIS. Well, but as we sit here, can you think of any privilege that would preclude the Committee?

Mr. MUELLER. Deliberative. Deliberative.

Mr. DAVIS. Okay. That is your answer.

Let me move forward. I think you have indicated that you did not encounter Mr. Gonzales or Mr. Card at the hospital. Is that right?

Mr. MUELLER. Correct.

Mr. DAVIS. But you did speak with Mr. Ashcroft after the conversation that he had with Mr. Card and Mr. Gonzales. Is that right?

Mr. MUELLER. I did.

Mr. DAVIS. Did you make any notes regarding your conversation with Mr. Ashcroft?

Mr. MUELLER. Yes.

Mr. DAVIS. And do you still have those notes in your possession?

Mr. MUELLER. Yes.

Mr. DAVIS. Can you think of any reason why those notes should not be disclosed to the Committee?

Mr. MUELLER. The same response that I gave before in response to your earlier question, deliberative.

Mr. DAVIS. Now—this is an important question—tell me why you decided to make notes of your conversation with Mr. Ashcroft?

Mr. MUELLER. It was out of the ordinary.

Mr. DAVIS. What was out of the ordinary, Mr. Mueller?

Mr. MUELLER. Being asked to go to the hospital and be present at that time.

Mr. DAVIS. Did you share those notes with anyone in the Administration?

Mr. MUELLER. No.

Mr. DAVIS. Who have you shared them with prior to today?

Mr. MUELLER. My counsel.

Mr. DAVIS. Counsel——

Mr. MUELLER. Office of General Counsel.

Mr. DAVIS. Okay. Is that the only individual, Office of General Counsel?

Mr. MUELLER. Yes. Well, there may have been persons in my immediate staff, but——

Mr. DAVIS. Have you made any other notes or memorandum regarding the March 10 visit that you have characterized as unusual?

Mr. MUELLER. No.

Mr. DAVIS. Do you know if any notes or memorandum were made regarding the visit itself? I understand you didn't make them as you weren't there, but regarding the visit by Mr. Card and Mr. Gonzales to Mr. Ashcroft, do you know if there was any notetaker present.

Mr. MUELLER. I do not know.

Mr. DAVIS. I am sorry. Did you finish your answer? I am sorry.

Mr. MUELLER. I was going to anticipate your next question is I have not seen any such notes.

Mr. DAVIS. Okay, and——

Mr. CONYERS. I hate to tell the gentleman this, but with two other Members and the vote on, we are now really——

Mr. DAVIS. If you would just indulge me 10 seconds, Mr. Chairman, I would ask the Committee to take note of Mr. Mueller's very candid statement to us that he does have notes regarding this very important conversation, and I would ask the Senate to certainly be aware of it.

And I would certainly ask this Committee and our colleagues in the Senate to make a formal inquiry to obtain those thanks

Thank you for being candid, Mr. Mueller.

Mr. CONYERS. Thank you very much.

The Chair recognizes the gentlelady from Florida, Debbie Wasserman Schultz.

Ms. WASSERMAN SCHULTZ. Thank you, Mr. Chairman.

Director Mueller, I am going to change the subject and ask some questions related to the Internet and the ICAC task forces.

As you know, the Internet has facilitated an explosion of child exploitation. And Department of Justice officials testified before the Energy and Commerce Committee in the last Congress that there are hundreds of thousands of individuals trafficking in child pornography in the United States.

Everyone that I have talked to—from Mark Lunsford in Florida who is Jessica Lunsford's father, Marc Klaas, Polly Klaas's father in California and a number of other parents who have formed the Surviving Parents Coalition, to the National Coalition to Protect Children—everyone tells me that this problem is only getting worse and not better.

ROBERT S. MUELLER, III
DIRECTOR
FEDERAL BUREAU OF INVESTIGATION
BEFORE THE
JUDICIARY COMMITTEE ON OVERSIGHT OF THE
UNITED STATES HOUSE OF REPRESENTATIVES
JULY 26, 2007

Good afternoon Chairman Conyers, Representative Smith, and members of the Committee. I am pleased to be here today.

When I was sworn-in as the sixth Director of the FBI nearly six years ago, I was keenly aware of the need to address a number of management and administrative challenges facing the Bureau. However, the terrorist attacks of September 11, 2001, coupled with the emerging terrorist and criminal threats brought on by globalization and advances in technology, required far more changes than we anticipated. Indeed, we in the FBI have undergone unprecedented transformation in recent years. Today, the FBI is a stronger organization, combining greater intelligence and national security capabilities with a longstanding commitment to protecting the American people from both crime and terrorism, while upholding the Constitution and protecting civil liberties.

Today, I want to give you a brief sense of the FBI's current priorities, the changes we have made to meet our mission, and some of the challenges we are facing.

Changes in Structure and in the Way We Do Business

After the September 11th attacks on America, the FBI's priorities shifted dramatically. Our top priority became the prevention of another terrorist attack. Today, our top three priorities – counterterrorism, counterintelligence, and cyber security – are national security-related.

To that end, we have made a number of changes in the Bureau, both in structure and in the way we do business. We stood up the National Security Branch, which oversees our counterterrorism, counterintelligence, and intelligence operations. We consolidated our chemical, biological, radiological, and nuclear threat resources into the Weapons of Mass Destruction Directorate.

We have doubled the number of intelligence analysts on board, from 1,023 in September 2001 to more than 2,100 today. We have tripled the number of linguists. We set up Field Intelligence Groups, or FIGS, in each of our 56 field offices. These FIGS combine the expertise of agents, analysts, translators, and surveillance specialists. We integrated our intelligence program with other agencies under the Director of National Intelligence, with appropriate protections for privacy and civil liberties.

We have tripled the number of Joint Terrorism Task Forces (JTTFs) across the country, from 33 to more than 100. These task forces combine the resources of the FBI, the intelligence community, the military, and state and local police officers. These JTTFs have been essential in breaking up terrorist plots across the country, from Portland, Lackawanna, Torrance, and Chicago, to the recent Fort Dix and JFK plots.

In short, we have improved our national security capabilities across the board. Today, intelligence is woven throughout every program and every operation. Much of our progress has been the result of expertise gained over the past 99 years of our existence, in the criminal arena with organized crime, and in counterintelligence, through the development of sources and expertise in interview and surveillance techniques. Our experience has allowed us to build enhanced capabilities on an already strong foundation.

The FBI's Criminal Programs

To meet our national security mission, the FBI had to shift personnel and resources, but this has not affected our commitment to our significant criminal responsibilities. While Americans justifiably worry about terrorism, crime also touches the lives of millions of people. Today in the FBI, we have roughly a 50/50 split in resources between national security and criminal programs. To make the best use of these resources, we will continue to focus on those areas where we bring something unique to the table and to target those criminal threats against which we will have the most substantial and lasting impact.

In recent years, we have moved away from traditional drug cases and smaller white collar crimes that can be handled by other law enforcement agencies, but we have dedicated more agents and more resources to public corruption, violent crime, civil rights, transnational organized crime, corporate fraud, and crimes against children. We remain ready and willing to help keep our communities safe.

Public Corruption

Public Corruption is among the agency's top priorities and is the number one priority of the Criminal Investigative Division. Public corruption strikes at the heart of government. It erodes public confidence, and undermines the strength of our democracy. Investigating public corruption is an FBI commitment as old as the Bureau itself. Indeed, it is a mission for which the FBI is singularly situated; we have the skills necessary to conduct undercover operations and the ability to perform electronic surveillance.

Today, there are 640 Special Agents dedicated to more than 2,400 pending investigations. The number of pending cases has increased by 49 percent since 2001. The number of agents working such cases has increased by 42 percent. The Department of Justice's conviction rate is high, as is the overall number of corruption convictions. In the past two years alone, the Department has convicted over 1,500 federal, state, and local officials. The Department also has recovered more than $69 million in fines and more than $356 million in restitution.

The Public Corruption Program also targets governmental fraud and corrupt practices. For example, the International Contract Corruption Initiative addresses the systemic, long-term multi-billion dollar contract corruption and procurement fraud crime problem in the Middle East, principally in Iraq, Kuwait, and Afghanistan.

The Hurricane Fraud Initiative addresses contract and procurement fraud in the Gulf Coast region of the United States in the aftermath of hurricanes Katrina and Rita. The Campaign Finance and Ballot Fraud Initiative addresses campaign finance violations, with a particular emphasis on the upcoming 2008 primaries and national elections.

Violent Crime

National crime rates remain near historic lows, thanks in large part to the courageous efforts of local, state and federal law enforcement agencies, and several major metropolitan areas continue to report decreases in the number of violent crimes in their communities. Nevertheless, it must be acknowledged that the FBI's 2005 Uniform Crime Report (UCR) and the 2006 preliminary UCR did signal a slight increase in the aggregate number of violent crimes in America. These data do not reveal a nationwide trend; instead, they show local increases in some violent crimes in certain communities.

Despite the continuation of historically low crime rates, the Department of Justice and the FBI take seriously any increase in crime, and here, too, we strive to maximize our resources through partnerships and task forces. We are currently operating 188 Safe Streets Task Forces. Forty-three of these task forces are dedicated to violent crime; 10 are dedicated to major theft. In addition, there are 16 Safe Trails Task Forces that cover crimes committed in Indian Country such as homicide, rape, child sexual assault, and narcotics trafficking. Task forces dedicated to violent crime alone conducted investigations resulting in more than 700 convictions in Fiscal Year 2006.

We also participate in state and local fusion centers across the country. More than 250 Special Agents, analysts, and linguists work side-by-side with their state and local counterparts, collecting intelligence, analyzing criminal trends, and sharing that information up and down the line, from federal and state officials to the officer on the street.

We are also working together to combat crimes against children. The Innocence Lost National Initiative works to identify and disrupt child prostitution rings. To date, the program has been expanded to 29 cities, with 23 dedicated task forces and working groups. Since its inception, more than 300 children have been recovered and/or identified, and 204 child predators have been convicted in federal or state court.

To address the pervasive problem of child abductions, the FBI created the Child Abduction Rapid Deployment (CARD) teams. There are currently 10 teams regionally dispersed to enable the rapid deployment of experienced Crimes Against Children investigators. These agents provide investigative, technical, and resource assistance to state and local law enforcement during the most critical time period after a child is abducted. Since April 2006, the CARD teams have been deployed 23 times. Eleven victims have been recovered alive and all but two investigations have been resolved.

Violent Gang Activity

We also face significant challenges from violent gangs. They are a nationwide plague that is no longer limited to our largest cities.

Since 2001, for example, our violent gang caseload has more than doubled. Currently, we have more than 2,800 pending investigations into gangs and gang-related activities. The number of agents working such cases has increased by 70 percent.

We routinely work with our state and local partners to combat this pervasive threat. Of our 188 Safe Streets Task Forces, 135 are dedicated to identifying, prioritizing, and targeting violent gangs. We now have more than 600 agents serving on those task forces, along with more than 1,100 officers from state and local law enforcement. Last year, they convicted nearly 2,200 violent gang members.

In addition to our task force participation, we stood up the National Gang Intelligence Center (NGIC) in Washington, D.C. to support our law enforcement partners on the front lines. The NGIC shares information and analysis concerning the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities across the United States. The NGIC is co-located with GangTECC, the National Gang Targeting, Enforcement and Coordination Center, which is the national, multi-agency anti-gang task force created by the Attorney General. The MS-13 National Gang Task Force supports FBI field office investigations of the MS-13 international gang, and coordinates investigations with other local, state, federal, and international criminal justice agencies.

In support of the President's strategy to combat criminal gangs from Central America and Mexico, the FBI has forged partnerships with anti-gang officials in El Salvador, Honduras, and Guatemala, among other countries. We are working with the U.S. Department of State and the Department of Homeland Security to support the FBI's Central American Fingerprint Exploitation (CAFE) initiative, which collects gang members' fingerprints in the above-referenced countries, allowing the United States to deny entry to the country even if they utilize aliases, and the new Transnational Anti-Gang (TAG) Center announced by the Attorney General in San Salvador in February.

Civil Rights Program

As you know, the FBI is charged with investigating civil rights violations. In recent years, we have expanded our Civil Rights Program beyond police brutality and hate crimes, to include the Civil Rights Cold Case Initiative and human trafficking issues. Since 2001, the number of pending civil rights cases has increased 19 percent, from 1,326 to 1,587.

In February of 2006, the FBI and the Department of Justice began to work with the NAACP, the Southern Poverty Law Center, and the National Urban League on the Civil Rights Cold Case Initiative. As part of this initiative, the FBI asked its 56 field offices to re-examine their unsolved civil rights cases, and to determine which cases could still be viable for prosecution. Since this initiative began, 95 referrals have been forwarded to 17 field offices. Each will need to be assessed for its investigative and legal viability, but for those cases in which we can move forward, we will.

We all know that many murders during the Civil Rights era were not fully investigated, were covered up, or were misidentified as accidental deaths or disappearances. Many trails ran cold, and many cases were effectively closed.

Yet the families and friends of these victims never lost hope, and breakthroughs in forensic analysis technology have affirmed that hope. In June of this year, for example, James Seale, a former member of the Ku Klux Klan, was convicted of the kidnapping and murder of Henry Dee and Charlie Moore back in 1964. In 2005, Edgar Ray Killen was convicted for his role in the deaths of three civil rights workers in Mississippi in 1964. And in 2003, Ernest Avants was convicted for the 1966 murder of Ben Chester White.

Through your support of these investigations, with the passage of the Emmett Till Unsolved Civil Rights Crime Act, we will have the resources we need to investigate and prosecute these crimes, and bring those responsible to justice.

Transnational Organized Crime

Transnational organized crime continues to evolve with advances in globalization and technology.

La Cosa Nostra is an organized crime enterprise with direct ties to the Sicilian Mafia and remains a major organized criminal threat to American society. Currently, we have nearly 600 pending Italian organized crime investigations. We are also actively investigating Eurasian, Albanian, Asian, and African organized criminal syndicates. Between 2001 and 2007, for example, pending Eurasian organized crime cases increased by 65 percent and an average of 160 individuals were indicted per year between 2002 and 2006.

We are working with partners around the world to identify, apprehend, and disrupt members of international criminal syndicates. For example, we are working with the Italian National Police to combat Sicilian Mafia activity in Italy and in the United States, in a partnership known as the Pantheon Project. The FBI has assigned personnel in Rome to work side-by-side with Italian National Police investigators, and the Italian National Police have assigned a representative to FBI Headquarters to work side-by-side with Agents in the Organized Crime Section.

The FBI-Hungarian National Police Organized Crime Task Force has been up and running for more than six years, working to dismantle organized crime groups, with FBI agents permanently stationed in Budapest to work with their Hungarian counterparts. The Albanian Organized Crime Task Force will commence operations this fall, with partial funding from the Department of Defense.

The FBI's Criminal Division has also assumed administrative and operational responsibility from the Office of International Operations for the Southeast European Cooperative Initiative (SECI), which is headquartered in Bucharest, Romania. SECI serves as a clearinghouse for information and intelligence for member and observer countries, and supports specialized task forces addressing transborder crimes including human trafficking, financial crimes, smuggling of goods and terrorism.

Recognizing the growing threat posed by transnational criminal enterprises throughout the world, the FBI, in conjunction with the Department of Justice, has begun an assessment of the world-wide organized crime threat. This collaborative effort between the United States, Great Britain, Canada, Australia, and New Zealand will enable us to focus resources internationally in order to neutralize those organized crime groups with the greatest impact and longest reach.

Major White Collar Crime

The FBI routinely investigates large-scale financial crimes, including corporate, securities, commodities, mortgage and health care fraud. In recent years, the FBI has investigated company after company, including Enron, Enterasys, Comverse, HealthSouth, WorldCom, and Qwest, among many others. These names have been in the headlines for the past several years. Thousands of employees lost their jobs and their life savings; thousands of stockholders were defrauded. We have successfully investigated and helped put away many of the persons responsible for these crimes.

The number of agents investigating corporate and other securities, commodities, and investment fraud cases has increased 47 percent, from 177 in 2001 to more than 250 today. Today, we have more than 1,700 pending corporate, securities, commodities and investment fraud cases, which is an increase of 37 percent since 2001.

In 2006, the FBI investigated 490 corporate fraud cases, resulting in 176 informations and indictments, 133 convictions, $14 million in fines, and $62 million in seized assets. Significantly, the FBI has also secured $1.2 billion in court ordered restitution for the victims of these crimes.

We are also a member of the Corporate Fraud Task Force. FBI Special Agents work closely with investigators from the Securities & Exchange Commission, the IRS, the U.S. Postal Inspection Service, the Commodity Futures Trading Commission, and Treasury's Financial Crimes Enforcement Network, among others. Together, we target sophisticated, multi-layered fraud cases that injure the marketplace and threaten our economy. Since its inception, the Department has obtained 1,236 corporate fraud convictions, including the convictions of 214 chief executive officers and presidents, and 53 chief financial officers.

Health care fraud significantly impacts the lives of all Americans. The National Health Care Anti-Fraud Association conservatively estimates that three to five percent of total health care expenses are fraudulent. The major issues are constantly changing and those involved in health care fraud are continually probing health care benefits programs for areas of potential fraud. Constant communication between the health care benefits programs, law enforcement agencies, state agencies and the public is the most effective means to respond to these changes. The FBI is an integral element of the joint Department of Justice and Department of Health and Human Services Health Care Fraud and Abuse Program and is actively involved in 32 Health Care Fraud Task Forces, as well as numerous working groups and joint investigations. During 2006, investigations resulted in 599 indictments; 534 convictions and pre-trial diversions; $373 million in restitutions; and $1.6 billion in recoveries.

Cyber Crime

Protecting the United States against cyber-based attacks and high-technology crimes is our third priority, ranking behind only counterterrorism and counterintelligence. With the ubiquitous nature of the Internet, cyber crime is an ever-evolving threat. Our foreign adversaries and competitors can remotely observe, target, acquire and exploit our information to their advantage, often without any physical presence in the United States. Terrorists recruit, train and plan attacks in the shadows of the Internet. Sexual predators prowl chat rooms for younger and younger victims. Spies sell intellectual property and state secrets to the highest bidder. Hackers who used to shut down servers around the world for bragging rights may be linked to criminal or terrorist organizations. In addition, many traditional crimes, from money laundering and fraud to identity theft and organized crime, have migrated online.

Five years ago, in 2002, we created the Cyber Division to handle all cyber-security crimes. Today, our highly-trained cyber agents and analysts investigate computer fraud, child exploitation, theft of intellectual property, and worldwide computer intrusions.

Innocent Images National Initiative

One of our most important cyber programs is the Innocent Images National Initiative (IINI). The IINI is an intelligence-driven, multi-agency investigative operation to combat the proliferation of Internet child pornography and exploitation. Unfortunately, there is no shortage of work in this arena. In the past 10 years, we have witnessed an exponential increase in our caseload, from just 113 cases in 1996 to more than 5,000 this year. In fact, online child pornography and exploitation investigations accounted for 37 percent of all investigations in the Cyber Division in Fiscal Year 2006. In total, more than 6,000 child predators have been convicted in FBI cases since 1996.

We have ongoing undercover operations across the country, with hundreds of agents who investigate cases with their state and local counterparts. On any given day, these investigators may pose as children to lure online predators into the open. They may pose as collectors who seek to share images through peer-to-peer networks. They may coordinate with the National Center for Missing and Exploited Children to identify children and adults featured in child pornography. Or they may train police officers to investigate cases in their own jurisdictions.

Our collaboration is not limited to the national level. Many producers and distributors of child pornography operate outside of our borders. Police officers from Britain, Australia, Belarus, Thailand, and the Philippines, among others, work with agents and analysts on the Innocent Images International Task Force in Calverton, Maryland. Since its inception, investigators from 19 countries have participated in the task force. Together, they have generated more than 3,000 leads that were sent to DOJ-funded Internet Crimes Against Children Task Forces, FBI field offices, and our international law enforcement partners.

Online Fraud, Cyber Espionage, and Computer Intrusions

We also investigate online fraud, identity theft, intellectual property violations, cyber espionage, and computer intrusions.

For example, an ongoing cyber crime initiative has identified more than one million potential victims of botnet cyber crime. The investigation, entitled "Operation Bot Roast," targets "botnets" – groups of compromised computers under the remote command and control of a hacker commonly known as a "bot-herder."

Most owners of these compromised computers are unwitting victims who have unintentionally allowed access and use of their computers to facilitate other crimes, including identity theft, denial of service attacks, phishing, click fraud, and the mass distribution of spam and spyware. Because of their widely distributed capabilities, botnets are a growing threat to national security, the national information infrastructure, and the economy.

The FBI is working with industry partners like the CERT Coordination Center at Carnegie Mellon University, Microsoft Corporation, and the Botnet Task Force to identify victim computer IP addresses and to notify those affected. To date, several suspects have been charged or arrested with computer fraud and abuse.

The FBI sponsors InfraGard, a cutting edge public and private alliance committed to information sharing and analysis to combine the knowledge base of a wide range of members. InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard Chapters are geographically linked with FBI Field Office territories. Currently, there are over 20,000 individual Infraguard members, representing 240 Fortune 500 companies and all National Critical Infrastructure sectors.

Increasingly, cyber threats originate outside of the United States. Our information infrastructure is not ours alone – it can be accessed by anyone with a laptop and a modem. Our Cyber Action Teams travel around the world on a moment's notice to assist in computer intrusion cases, whether in government, military, or commercial systems. These teams gather vital intelligence that helps us identify the cyber crimes that are most dangerous to our national security and to our economy.

In 2005, for example, cyber teams comprising investigators and experts in malicious code and computer forensics worked closely with Microsoft Corporation and with law enforcement officials from Turkey and Morocco to find the criminals responsible for creating and spreading the "Mytob" and "Zotob" worms. We resolved this case within just weeks of the attack, in large part because of the intelligence we received from our international and private sector partners.

We are also uniquely positioned to investigate counterintelligence threats in the cyber arena. Although I am limited in what I can discuss in an open forum, the FBI is partnered in the National Cyber Investigative Joint Task Force with elements of the Intelligence Community to investigate and respond to counterintelligence cyber threats.

International Scope and Operations

In today's "flat world," our role cannot be limited to the domestic front. Just as there are no borders for crime and terrorism, there can be no borders for justice and the rule of law.

To respond to this new threat landscape, the FBI must create new partnerships and solidify old friendships with our counterparts around the world. Twenty years ago, the idea of regularly communicating with our law enforcement and intelligence counterparts around the world was as foreign as the Internet or the mobile phone. Today, advances in technology, travel, and communication have broken down walls between countries, continents, and individuals.

To that end, we have strengthened our relationships with our international law enforcement partners; we have expanded our global reach. The FBI now has Legal Attaché offices – called Legats – in more than 70 cities around the world, providing coverage for more than 200 countries.

These Legats are the FBI's first responders on the global front, from assisting our British counterparts in the London bombings to finding the man responsible for the attempted assassination of President Bush in Tbilisi, Georgia. We train together; we work hand-in-hand on multinational task forces and investigations. We have assisted counterterrorism investigations from Saudi Arabia to Spain, and from Britain to Bali.

Together we are identifying people and groups that provide financial support to terrorists. We are collaborating closely with our counterparts in Russia, Eastern Europe, and Asia to combat global nuclear terrorism. We are working with the Italian National Police and the Hungarian National Police to investigate organized criminal syndicates that continue to immigrate to the United States. We are working with our foreign counterparts to cut off the proliferation of child pornography on the Internet. These international partnerships are vital to our collective security.

National Security Letters and the Office of Integrity and Compliance

In response to the Inspector General's report dated March 9, 2007, concerning the FBI's use of National Security Letters (NSLs), and an internal audit conducted by the FBI, the Bureau is in the process of implementing numerous reforms. These reforms will ensure that we comply fully with both the letter and the spirit of the authorities entrusted to us.

We are conducting audits to identify and rectify errors in our use of NSLs. We are streamlining the approval process to include review of all NSL requests by FBI attorneys. We are training agents and supervisors how and when to use NSLs.

With regard to the collection of data, investigators must request specific information and justify the need for such information before the NSL is sent. In addition, all evidence received from an NSL must be reviewed before it is included in the FBI's databases, to ensure that only the information requested is retained. Any irrelevant data will be isolated from other data and may be returned or destroyed. Further, the use of so-called "exigent letters" is no longer permitted. New guidelines provide a clear process to be followed in cases of emergency. The FBI has also worked closely with the privacy and civil liberties officers of the Department of Justice and the Office of the Director of National Intelligence to insure that policies for retention of information obtained through NSLs are appropriate to protect privacy and civil liberties.

As part of a significant national security oversight and compliance effort, we are working with the Department of Justice as it stands up a dedicated Oversight Section within the National Security Division. This section will be comprised of attorneys and staff members specifically dedicated to ensuring that the Department of Justice fulfills its national security oversight responsibilities, to include all aspects of the FBI's national security program and its use of national security tools. The Department will exercise this oversight through a regular process of conducting National Security Reviews of FBI field offices and Headquarters national security units. These reviews are not limited to areas where shortcomings have been identified; instead, they are intended to enhance compliance across the national security investigative spectrum.

Finally, within the FBI itself, we have proposed establishment of the Office of Integrity and Compliance (OIC), which will soon be submitted to Congress and the Office of Management and Budget for their concurrence. After the Inspector General's audit of the FBI's use of NSLs brought to our attention an unacceptably high rate of error, we took a hard look at the causes. While we had training for the use of NSLs in place, we had no built-in, effective way to track compliance with those requirements.

While many large corporations have compliance divisions, few, if any, government agencies have department-wide programs to internally monitor compliance. Given the complex nature of the FBI's mission, as well as the number of rules, guidelines, and laws to which we are subject, it is time to start such a program. In developing this proposal, we have welcomed the input of the Privacy and Civil Liberties Oversight Board, external privacy and civil liberties groups, as well as Congress.

The OIC will develop, implement, and oversee a program that ensures there are processes and programs in place that promote FBI compliance with both the letter and the spirit of all applicable laws, regulations, rules, and policies. Through this program, we will cultivate an environment committed to these principles and will assist FBI management at all levels to maintain a culture where ethics and compliance are paramount considerations in decision making. The OIC will be headed by an Assistant Director who will report directly to the FBI's Deputy Director, providing direct access to the top decision makers within the FBI. The OIC will not duplicate the work of the Inspections Division, but will identify areas of risk so that we can mitigate the risk.

These comprehensive oversight and compliance programs will ensure that national security investigations are conducted in a manner consistent with our laws, regulations, and policies, including those designed to protect the privacy interests and civil liberties of American citizens. The FBI will do all that it can to uphold our core value of integrity in order to maintain public trust and confidence.

Information Technology

In recent years, we have made vast improvements to the FBI's outdated information technology systems. We have installed thousands of state-of-the-art computers and secure global networks. We have developed sophisticated databases and search engines, many of which we share with our federal, state, local and tribal counterparts.

We are also in the process of implementing Sentinel, our fully automated, web-based case management system. The Sentinel system, when completed, will help the FBI manage information beyond the case focus of existing systems, and will provide enhanced information sharing, search, and analysis capabilities. Sentinel also will facilitate information sharing with members of the law enforcement and intelligence communities.

In June, we implemented the first phase of Sentinel. Phase 1 provides a user-friendly, web-based interface to access information that is housed in the FBI's Automated Case Support (ACS) system. Information is pushed to users, and documents are made available through hyperlinks. Phase 1 features a Personal Workbox, which summarizes a user's cases and leads, putting more information at their fingertips. It also provides a Squad Workbox, which allows supervisors to better manage their resources and assign leads with the click of a mouse.

We are currently working with Lockheed Martin, the prime contractor, to plan the development and deployment of the next set of Sentinel capabilities. With Phase 1, we built the foundation for the entire enterprise. Phase 2 will add additional capabilities, such as electronic forms and electronic workflow, through which employees can send documents to supervisors for review, comment, and approval. Phase 2 is scheduled for incremental development and deployment, providing capabilities to users in a more timely fashion. The four-phase Sentinel project is scheduled to conclude in 2011, as originally planned.

Future of the FBI

The FBI was created nearly 100 years ago to address crime crossing state boundaries. Today, we combat crime and terrorism that cross state boundaries and national borders with the click of a mouse. The world is smaller and more interconnected than it ever has been. Unfortunately, criminals and terrorists are also more interconnected. The threats we face are global in nature, and the technology is moving more quickly than we could have foreseen just 10 years ago.

To defeat these emerging threats, we must continue to expand our global reach. We must continue to share information with our federal, state, local, tribal, and international partners. We must continue to update our technology to keep pace with criminals and terrorists the world over. We must continue to work together to dismantle criminal enterprises and terrorist cells, to put away child predators and violent gang members, and to disrupt criminals and terrorists before they strike. Working together is not just the **best** option; it is the **only** option.

Today, we are building on our legacy and our capabilities as we focus on our top priority: preventing another terrorist attack. It is indeed a time of change in the FBI, but our values can never change. We must continue to protect the security of our nation while upholding the civil rights guaranteed by the Constitution to every citizen.

When I speak to Special Agents upon their graduation from the FBI Academy, I remind each one that it is not enough to prevent foreign countries from stealing our secrets – we must prevent that from happening while still upholding the rule of law. It is not enough to stop the terrorist – we must stop him while maintaining his civil liberties. It is not enough to catch the criminal – we must catch him while respecting his civil rights. The rule of law, civil liberties, civil rights – these are not our burdens; they are what make us Americans.

* * *

Mr. Chairman, I would like to conclude by thanking this Committee and you for your service and your support. Many of the accomplishments we have realized during the past six years are in part due to your efforts. From addressing the growing gang problem to creating additional Legal Attaché offices around the world, to compensating our personnel, and, most importantly, to protecting the American people from terrorist attack, you have supported our efforts and our budget requests.

On behalf of the men and women of the FBI, I look forward to working with you in the years to come as we continue to develop the capabilities we need to defeat the threats of the future.

Exhibit 3

The Attorney General

Washington, D.C.

January 17, 2007

The Honorable Patrick Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

The Honorable Arlen Specter
Ranking Minority Member
Committee of the Judiciary
United States Senate
Washington, D.C. 20510

Dear Chairman Leahy and Senator Specter:

I am writing to inform you that on January 10, 2007, a Judge of the Foreign Intelligence Surveillance Court issued orders authorizing the Government to target for collection international communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. As a result of these orders, any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.

In the spring of 2005—well before the first press account disclosing the existence of the Terrorist Surveillance Program—the Administration began exploring options for seeking such FISA Court approval. Any court authorization had to ensure that the Intelligence Community would have the speed and agility necessary to protect the Nation from al Qaeda—the very speed and agility that was offered by the Terrorist Surveillance Program. These orders are innovative, they are complex, and it took considerable time and work for the Government to develop the approach that was proposed to the Court and for the Judge on the FISC to consider and approve these orders.

The President is committed to using all lawful tools to protect our Nation from the terrorist threat, including making maximum use of the authorities provided by FISA and taking full advantage of developments in the law. Although, as we have previously explained, the Terrorist Surveillance Program fully complies with the law, the orders the Government has obtained will allow the necessary speed and agility while providing substantial advantages. Accordingly, under these circumstances, the President has determined not to reauthorize the Terrorist Surveillance Program when the current authorization expires.

The Intelligence Committees have been briefed on the highly classified details of these orders. In addition, I have directed Steve Bradbury, Acting Assistant Attorney General for the Office of Legal Counsel, and Ken Wainstein, Assistant Attorney General for National Security, to provide a classified briefing to you on the details of these orders.

Sincerely,

Alberto R. Gonzales
Attorney General

cc: The Honorable John D. Rockefeller, IV
The Honorable Christopher Bond
The Honorable Sylvester Reyes
The Honorable Peter Hoekstra
The Honorable John Conyers, Jr.
The Honorable Lamar S. Smith

Exhibit 4

HEARING OF THE SENATE SELECT COMMITTEE ON INTELLIGENCE
PROPOSED FISA MODERNIZATION LEGISLATION

WITNESSES:

MR. MIKE McCONNELL, DIRECTOR OF NATIONAL INTELLIGENCE;

LTG KEITH ALEXANDER, DIRECTOR, NATIONAL SECURITY AGENCY;

MR. KENNETH WAINSTEIN, ASSISTANT ATTORNEY GENERAL FOR NATIONAL SECURITY, DEPARTMENT OF JUSTICE;

MR. BENJAMIN POWELL, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE;

MR. VITO POTENZA, GENERAL COUNSEL, NATIONAL SECURITY AGENCY

CHAIRED BY: SENATOR JOHN D. ROCKEFELLER IV (D-WV)

LOCATION: 106 DIRKSEN SENATE OFFICE BUILDING, WASHINGTON, D.C.

TIME: 2:30 P.M. EDT
DATE: TUESDAY, MAY 1, 2007

SEN. ROCKEFELLER: This hearing has begun, and I welcome all of our testifiers. And other members of the committee will be coming in. I know some of the caucuses just broke up.

The Select Committee on Intelligence meets today in open session, something we don't ought to do, to consider whether the scope and application regarding the Surveillance Act needs to changed to reflect the evolving needs for the timely collection of foreign intelligence. An extraordinarily complicated subject, this is. At the committee's request, the administration has undertaken a comprehensive review of the Foreign Intelligence Surveillance Act, commonly referred to as FISA. Out of this review, the administration proposed -- it believes would modernize the laws governing the way in which we gather foreign intelligence with the use of electronic surveillance.

Consideration of the administration's proposal and alternatives will be rooted in the Intelligence Committee's 30-year experience with our nation's long and delicate effort to strike that elusive right balance between effective intelligence collection for our national security and the constitutional rights and privacy interests of Americans.

The Intelligence Committee's existence came out of the work of the Church Committee and others in the mid-'70s to bring to light abuses in the electronic surveillance of Americans. One of the committee's first tasks was to work with the Senate Judiciary Committee and with the Ford and Carter administrations from 1976 to 1978 to enact the Foreign Intelligence Surveillance Act. As we take a fresh look at the current law, we will again be working with our colleagues in the Senate Judiciary Committee.

FISA involves both the judicial process on the one hand and the collection of intelligence. Our committee's contribution to this process will be our ability to assess the relationship between the public realm of legislative reforms and the classified realm of intelligence collection. By necessity, much of the committee's assessment must occur in a classified setting; yet most of what we do, in contrast to the Judiciary Committee, will occur in closed session, I believe it is important to hold our hearing today in open session.

The purpose of today's hearing is to enable the administration to explain to the Senate and to the American people as openly as possible the reasons why public law on these vital matters should be changed.

I would like to make a few observations about the administration's legislative proposal before us.

One part of the administration's bill proposes to terminate controversies now in litigation in various courts arising from the warrantless surveillance program that the president has labeled "the Terrorist Surveillance Program." It would bar any lawsuit against any person for the alleged provision to any element of the intelligence community's information or assistance for any alleged communications intelligence activity.

Under the administration's proposal, this immunity provision would be limited to alleged assistance from September 11th, 2001, to 90 days after enactment of any change in the law, were there to be one. We will carefully examine this immunity process and proposal and possible alternatives to it -- it is not without controversy -- as we will all sections of the administration bill. But I do believe that the administration is going to have to do its part, too.

The vice chairman and I have stressed to the administration repeatedly that the committee must receive complete information about the president's surveillance program in order to consider legislation in this area. This is a matter of common sense -- cannot legislate in the blind. We have made some progress towards that end, but there are key pieces of requested information that the committee needs and has not yet received.

These include the president's authorizations for the program, and the Department of Justice's opinion on the legality of the program. My request for these documents is over a year in length, and Vice Chairman Bond and I restated the importance of receiving these documents in our March letter, that in fact called this hearing. The administration's delay in providing these basic documents is incomprehensible, I think, inexcusable, and serves only to hamper the committee's ability to consider the liability of the Defense proposal before it -- inadequate information.

Congress is being asked to enact legislation that brings to end lawsuits that allege violations of the rights of Americans. In considering that request, it is essential that the committee know whether all involved, government officials and anyone else, relied on sound, legal conclusions of the government's highest law officer. The opinions of the attorney general are not just private advice. They are an authoritative statement of law within the executive branch.

From our government's beginning in 1789 until 1982, there had been 43 published volumes of opinions of attorney generals. Since then there have been 24 published volumes of the opinions of DOJ's Office of Legal Counsel.

From time to time, of necessity, a few will be classified. While those cannot be published, they can and should be provided to the congressional intelligence committees. We're in the classified business too, and we stick to it. There is simply no excuse for not providing to this committee all of the legal opinions on the president's program.

The administration's proposal to modernize FISA, if enacted, would be the most significant change to the statute since its enactment in 1978. It will be our duty to carefully scrutinize these proposed changes and ask many questions. And let me identify three.

First, from the beginning, FISA has required the approval of the FISA Court for the conduct of electronic surveillance done by wiretapping, quote, "in," end quote, the United States of America of communications, quote, "to or from," end quote, a person in the United States. The Judiciary Committee explained in its 1977 report to the Senate that this covers the wiretapping in the United States of the international communications of persons in the United States. The administration would eliminate that requirement from the definition of electronic surveillance. An important question is whether that change will give the attorney general authority, without a court warrant, to wiretap in the United States international communications that are to or from a person in the United States, most of whom will be United States citizens.

If so, what are the reasons for changing the judgment of the Congress in 1978 that a FISA order should be required for such wiretapping in the United States? How will that protect the private interests of U.S. citizens and permanent residents in their international communications?

Second, the administration proposal would expand the power of the attorney general to order the assistance of private parties, without first obtaining a judicial FISA warrant that is based on the probable cause requirements in the present law. A limited form of judicial review will be available after those orders are issues. Although there are exceptions, our American legal tradition does not generally give our attorney general the power to give such orders. Instead, it gives the attorney general the power to go to the courts and ask for such orders. If the administration's proposal necessarily -- I mean, is it necessary, period? And does it take a step further down a path that we will regret as a nation?

Thirdly, the attorney general announced in January that the administration had replaced the president's surveillance program with the orders of the FISA court. While many of my colleagues believe that the president's program should have been placed under court review and authorization much earlier, it was nonetheless good news. The question that we must now ask is whether just months after that important development, any part of the administration's bill will enable the president to resume warrantless collection with this legislation as the statutory basis for so doing.

Before turning to the vice chairman for his opening statement, I make a concluding remark or so. The administration proposal was submitted to us by the director of National Intelligence, director Mike McConnell, who will take the lead in presenting it to us today. The leadership of the DNI in this matter is a positive example of reform at work, and we welcome it.

General Keith Alexander, the director of the National Security Agency, is representing the National Security Agency here today. The NSA, people should know, has a limited ability to speak for itself in public, but we can, the rest of us, and so I'd like to share this thought with my colleagues and with the American public.

NSA does not make the rules. It has no wish to do so. Congress sets policy for the NSA in law, and the president issues directives that the NSA must follow. Every American should have confidence, as we do from our close observation of this important truth, that the ranks of the NSA are filled with dedicated and honorable people who are committed to protecting this nation while scrupulously following the laws and procedures designed to protect the rights and liberties of Americans.

Also on our panel is Keith Wainstein, the assistant attorney general for national security. He is the first to hold that newly created position. He has that for the first time. In our preparation for our hearing and other matters in recent months, we have been aided enormously by key personnel in his division as well as the Office of Legal Counsel.

Finally, the main purpose of today's hearing is to give the administration a chance to place on the public record its proposal for change in public law. We also have invited interested members of the public, particularly individuals or organizations who have assisted the Congress from time to time with their views on FISA matters, to submit statements for our record about these legislative proposals.

I now turn to our distinguished vice chairman, Senator Bond.

SEN. CHRISTOPHER BOND (R-MO): Thank you very much, Mr. Chairman. I join with you in welcoming the panelists and to say how gratifying it is to see the intelligence community coming together working in a much more collaborative mood, an attitude that is very helpful.

We wish only that we could have the legislative structure that would facilitate such a cooperative working, and I join with you, having visited NSA, in paying the highest respect and regards to the work of the people at the NSA.

Since September 11th, we've fought a myriad of enemies united in their ideological hatred of America -- agile, widespread, technologically advanced. To prevail against them, our intelligence community needs tools that are flexible and can meet changing threats and circumstances. The purpose of today's hearing is to discuss whether the current statute provides enough flexibility, and if not, how do we update it.

Before I address serious aspects of the administration's proposal, let me share some concerns about holding this particular hearing in a public setting before this committee covers this issue behind closed doors.

The issue of FISA Modernization has come to the fore because of the very unfortunate public disclosure of the president's highly classified Terrorist Surveillance Program. Our committee has been engaged in the oversight of the president's program since its inception, and now every member of this committee, as I think they should, and an increased number of staff are read into the program, and we appreciate the clearance that has been expanded.

But as I've said before, the early warning system that is now under FISA is essential to defeating our enemies who are determined to inflict grave harm upon our citizens and upon the infrastructure of this nation. I believe that having an open hearing before a closed hearing is not advisable, and I've given the chairman recommendations in this regard.

Other committees, like the Senate Judiciary Committee, have already considered aspects of this issue in open session because they were looking at it from a judicial point of view. Those members were not read in, for the most part, to the president's program. Our committee looks at the issue from an intelligence and operational point of view, and are members therefore are read into the program.

There are several key reasons why I believe that proceeding first in open session is inadvisable. First, this is an area where there is a very fine line between what is classified, sensitive or just shouldn't be highlighted in public.

Second, we've put witnesses before us in a bad position when they may be unable to respond to our question because the best responses are classified, including the best reasons to justify the new legislation they are proposing.

Third, although members of this committee will go to a closed session and likely be satisfied with classified answers, the public may be left with the false impression that either the witnesses are not forthcoming or not fully answering our questions or even have good arguments. Worse yet, and with this topic in particular, if one of us were to make an honest mistake in wandering into sensitive territory, we could risk public exposure of vital intelligence collection methods that would significantly harm our intelligence capabilities.

Please don't understand (sic) me, Mr. Chairman. I have confidence in our membership. However, I believe one of the reasons our committee was created was to explore sensitive areas of national intelligence, to hash them out behind closed doors and to determine the best way to discuss them publicly, and then proceed with the public statements and report of -- on them responsibly to the Senate with unclassified legislation.

And as the chairman said, I believe that it is very important that there be a public discussion, and I agree with the chairman that that is a significant element. But I am troubled by proceeding first in public with a very sensitive national intelligence matter. I think we could serve our constituents and our national interests and the witnesses before us, ourselves and the American people if we had first proceeded in closed session. But that issue has been resolved.

I would caution, however, that all of us, members and witnesses, will have to be especially diligent to ensure that questions and responses do not reveal any classified or sensitive information. And we all share that responsibility. And I would encourage the witnesses that we understand you're not trying to be less than forthcoming if you reserve answers to a later closed session.

Turning now to the subject at hand, to examine the FISA statute, the administration has offered some important suggestions. And I expect that our witnesses will tell us why the changes are necessary and answer questions.

For instance, the administration proposed to update the definition for the term "electronic surveillance" that will make it technology-neutral, unlike the current definition, which makes distinctions between wire, radio and other communications. The administration proposal would modify the time period for emergency authorizations from 72 to 168 hours, to ease the strain on vital resources within the Department of Justice and the FBI.

A long-overdue change is to update the FISA definition of the term "contents" to make it consistent with the definition used by the FISA pen register provision and the criminal wiretap statute. It simply makes no sense to have two different definitions for the same term in the same statute.

An important -- another important improvement is to streamline FISA applications and orders. This streamlining would be consistent with one of the recommendations this committee's staff audit made on the FISA project in 2005.

In summary, these are just some of the important issues we're going to discuss today. And we must remember that change simply for change's sake is not the goal. Ensuring the collection capabilities of our intelligence community now and in the future should be the goal.

As we learned from the events of September 11th, what we do here will have lasting effects not just on our intelligence sources and methods, but on our country's security.

Mr. Chairman, I'm sure that all of us look forward to a full and frank discussion about FISA modernization, the administration's proposal, and the impact on our sources and methods. Our witnesses have considerable experience and credibility in matters of national security and intelligence, and I look forward to hearing their opinions.

I do understand the public interest in this subject, and I'll have some questions for the administration during open session. However, as any full discussion will involve classified intelligence sources and methods, I would urge all my colleagues to exercise extra care in their questions and comments this afternoon.

With that, Mr. Chairman, I thank you for holding the hearing, and I look forward to hearing from our witnesses.

SEN. ROCKEFELLER: Thank you. I appreciate your comments very much, and I join you in always the concern of crossing the line. I do think it's important, however, that assuming that we can discipline ourselves not to cross the line, which I fully believe, I certainly know that you all can, and I certainly think that we can, that having this put before the American public in broad terms is useful, and then we go after it in a more vigorous way in closed session.

Having said that, Director McConnell, please proceed.

MR. MIKE McCONNELL: Good afternoon, Chairman Rockefeller, Vice Chairman Bond, members of the committee. Thank you for inviting us to come today to engage with the Congress on legislation that will modernize the Foreign Intelligence Surveillance Act, as you mentioned, FISA -- I'll refer to it as FISA from this point on -- which was passed in 1978.

In response to your guidance from last year on the need to revise FISA, the administration has worked for over the past year, with many of you and your staff experts, to craft the proposed legislative draft. It will help our intelligence professionals, if passed, protect the nation by preventing terrorist acts inside the United States. Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers or agents of foreign powers inside the United States. We are here today to share with you the criticality -- critical important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the civil and the privacy rights of all Americans.

The proposed legislation to amend FISA has four key characteristics. First, it makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978. Second, it seeks to restore FISA to its original focus on protecting the privacy interests of persons inside the United States. Third, it enhances the government's authority to secure assistance by private entities, which is vital for the intelligence community to be successful. And fourth, it makes changes that will streamline FISA administrative processes so that the intelligence community can use FISA as a tool to gather foreign intelligence information more quickly and more effectively.

The four critical questions, four critical questions that we must address in collection against foreign powers or agents of foreign powers are the following. First, who is the target of the communications? Second, where is the target located? Third, how do we intercept the communications? And fourth, where do we intercept the communications? Where we intercept the communications has become a very important part of the determination that must be considered in updating FISA.

As the committee is aware, I've spent the majority of my professional life in or serving the intelligence community. In that capacity, I've been both a collector of information and a consumer of intelligence information. I had the honor of serving as the director of the National Security Agency from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function enabling the collection of foreign intelligence information.

In my first 10 weeks on the job as the new director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. The threats faced by our nation, as I have previously testified to this committee, are very complex and there are very many. I cannot overstate how instrumental FISA has been in helping the intelligence community protect the nation from terrorist attacks since September 11th, 2001.

Some of the specifics that support my testimony, as has been mentioned, cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose the capability if known to the terrorists. I look forward to elaborating further on aspects of the issues in a closed session that is scheduled to follow.

I can, however, make the following summary-level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the intelligence community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States.

Let me repeat that for emphasis. We are significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation. In today's threat environment, the FISA legislation is not agile enough to handle the community's and the country's intelligence needs. Enacted nearly 30 years ago, it has not kept pace with 21st century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S. -- that is, foreign -- persons located outside the United States.

Let me repeat again for emphasis. As a result, today's FISA requires judicial authorization to collect communications of non-U.S. persons -- i.e., foreigners -- located outside the United States. This clogs the FISA process with matters that have little to do with protecting civil liberties or privacy of persons in the United States. Modernizing FISA would greatly improve that process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail and before the internet was a tool used by hundreds of millions of people worldwide every day.

There are two kinds of communications. It's important to just recapture the fact, two kinds of communications: wire and wireless. It's either on a wire -- could be a copper wire, a fiber wire -- it's on a wire or it's wireless, meaning it's transmitted through the atmosphere.

When the law was passed in 1978, almost all local calls were on a wire. Almost all local calls, meaning in the United States, were on a wire, and almost all long-haul communications were in the air, were known as wireless communications. Therefore, FISA in 1978 was written to distinguish between collection on a wire and collection out of the air or against wireless.

Now in the age of modern communications today, the situation is completely reversed. It's completely reversed. Most long-haul communications -- think overseas -- are on a wire -- think fiberoptic pipe. And local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA, passed in 1978. Technological changes have brought within FISA's scope communications that we believe the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the act. And that is foreign-to-foreign communications by parties located overseas.

The solution is to make FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Additionally, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today, a single communication can transit the world even if the two people communicating are only located a few miles apart. And yet simply because our law has not kept pace with technology, communications intended to be excluded from FISA are in fact included. There is no real consequence -- this has real consequence on the intelligence community working to protect the nation.

Today intelligence agencies may apply, with the approval of the attorney general and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the intelligence community is often required to make a showing of probable cause.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the statutory requirement is to obtain a court order, based on a showing of probable cause, that slows, and in some cases prevents altogether, the government's effort to conduct surveillance of communications it believes are significant to national security, such as a terrorist coordinating attacks against the nation located overseas.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: when seeking to monitor foreign persons suspected of involvement in terrorist activity who are physically located in foreign countries, the intelligence community is required under today's FISA to obtain a court order to conduct surveillance. We find ourselves in a position, because of the language in the 1978 FISA statute, simply -- we have not kept pace with the revolution in communications technology that allows the flexibility we need.

As stated earlier, this committee and the American people should know that the information we are seeking is foreign intelligence information. Specifically, this includes information relating to the capabilities, intentions and activities of foreign powers or agents of foreign powers, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets while providing appropriate protection through court supervision to U.S. citizens and other persons located inside the United States.

Debates concerning the extent of the president's constitutional powers were heated in the mid-'70s, as indeed they are today. We believe that the judgment of the Congress at that time was that the FISA regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. Nothing -- and I would repeat -- nothing in the proposed legislation changes this basic premise in the law.

Additionally, this proposed legislation does not change the law or procedures governing how NSA or any other government agency treats information concerning U.S. or United States persons. For example, during the course of normal business under current law, NSA will sometimes -- and I repeat -- sometimes encounter information to, from or about a U.S. person; yet this fact does not in itself cause FISA to apply to NSA's overseas surveillance activities.

Instead, at all times, NSA applies procedures approved by the attorney general to minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure constitutional reasonableness of NSA's surveillance activities.

They eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence. The information is not targeted, stored, retained or used by the intelligence community.

Some observers may be concerned about reverse targeting. This could occur when a target of electronic surveillance is really a person inside the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, the intelligence community would and should be required to seek approval from the FISA Court in order undertake such electronic surveillance.

It is vitally important, as the proposed legislation reflects, that the government retain a means to secure the assistance of communications providers. As director of NSA, a private-sector consultant both to government and to industry, and as now the director of National Intelligence, I understand that it is in our interest and our job to provide the necessary support. To do that, we frequently need the sustained assistance of those outside the government to accomplish our mission.

Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the government to exercise electronic surveillance that is subject to court approval under FISA. However, the current FISA does not provide a comparable mechanism with respect to authorized communications intelligence activity. I'm differentiating between electronic surveillance and communications intelligence. The new legislative proposal would fill these gaps by providing the government with means to obtain the aid of a court to ensure private-sector cooperation with lawful intelligence activities and ensure protection of the private sector.

This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private- sector cooperation with the activities that are "electronic surveillance" under the current FISA but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the intelligence community in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA modernization proposal contains a provision that would accomplish this objective. When discussing whether significant changes to FISA are appropriate, it is useful to consider FISA's long history. Indeed, the catalysts of FISA's enactment were abuses of electronic surveillance that were brought to light in the mid-'70s.

The revelations of the Church and Pike committees resulted in new rules for United States intelligence agencies, rules meant to inhibit abuses while providing and protecting and allowing our intelligence capabilities to protect the nation.

I want to emphasize to this committee and to the American public that none of these changes, none of those being proposed, are intended to nor will they have the effect of disrupting the foundation of credibility and legitimacy of the FISA court, as established in 1978. Indeed, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the 1978 Church-Pike investigations and the enactment of the original FISA act.

Following the adoption of FISA, a wide-ranging new oversight structure was built into U.S. law. A series of laws and executive office orders established oversight procedures and substantive limitations on intelligence activities, appropriately so.

After FISA, this committee and its House counterpart were created. Oversight mechanisms were established within the Department of Justice and with each intelligence agency, including a system of inspectors general. More recently, additional protections have been implemented community-wide.

The Privacy and Civil Liberties Oversight Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004. This board advises the president and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations and executive branch policies related to efforts to protect the nation against terrorism.

Unlike in the 1970s, the intelligence community today operates with detailed, constitutionally-based, substantive and procedural limits under the watchful eyes of this Congress, numerous institutions within the executive branch and, through FISA, the judiciary.

The Judicial Joint Inquiry Commission into Intelligence Activities Before and After the Terrorist Attacks of September 11, 2001, recognized that there were systematic problems with FISA implementation. For example, the commission noted that "there were gaps in NSA's coverage of foreign communications and in FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and the intelligence community have continually sought ways to improve. The proposed changes to FISA address the problems noted by that commission.

Mr. Chairman, we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully and after extensive coordination for over a year. But for this work to succeed, this must be -- there must be bipartisan support for bringing FISA into the 21st century.

Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation.

I ask for your support in modernizing FISA so that we may continue to serve the nation for years to come.

As I stated before this committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's intelligence community, it is not only my desire but my duty to encourage changes to policies and procedures and, where needed, legislation to improve our ability to provide warning of terrorist activity and other threats to the nation. I look forward to answering the committee's questions regarding this important proposal to bring FISA into the 21st century.

SEN. ROCKEFELLER: Thank you, Mr. Director. That was forthright and informative, and we appreciate it.

Mr. Wainstein.

MR. KENNETH WAINSTEIN: Thank you. Chairman Rockefeller, Vice Chairman Bond and members of the committee, I want to thank you for this opportunity to testify about our proposal to modernize FISA. My colleagues and I have been working closely with this committee and your staff on this and several other FISA-related issues. And I want to express my appreciation on the part of all of us up here for your cooperative approach on these complicated and very important matters.

While the proposal before you today contains a number of important and needed improvements to the FISA process, I'd like to focus my opening statement on laying out the merits of one particular improvement that we're advocating, which is our proposal to revise the definition of electronic surveillance in the FISA statute. To do that I'll begin with a brief discussion of Congress's intent when it drafted FISA almost 30 years ago. I'll then address the sweeping changes in telecommunications technology that have caused the statute to deviate from its original purpose, so that it now covers many intelligence activities that Congress intended not to cover.

I will discuss how this unintended consequence has impaired our intelligence capabilities, and I'll urge you to modernize FISA to bring it back in line with its original purpose.

In enacting FISA back in 1978, Congress established a regime of judicial review and approval, and applied that regime to the government's foreign intelligence surveillance activities. But Congress applied that regime not as to all such activities, but only as to those that most substantially implicated the privacy interests of people in the United States. In defining the scope of the statute, Congress was sensitive to the importance of striking an appropriate balance between the protection of privacy on one hand and the collection of critical foreign intelligence information on the other. Congress struck that balance by designing a process that focused primarily on intelligence collection activities within the United States, where privacy interests are the most pronounced, and not on intelligence collection activities outside the United States, where cognizable privacy interests are minimal or non-existent.

Congress gave effect to this purpose through its careful definition of the statutory term "electronic surveillance," which is the term that identifies those collection activities that fall within the scope of the statute, and by implication, those that fall outside of it. Congress established this dichotomy by defining electronic surveillance by reference to the manner of the communication under surveillance, by distinguishing between wire communications, which, as the director said, were primarily the local and domestic traffic in 1978, and radio communications, which were primarily the international traffic of that era. Based on the communications reality of that time, that dichotomy more or less accomplished the congressional purpose of distinguishing between domestic communications which fell within FISA, and communications targeted at persons overseas which did not.

That reality has changed, however. It has changed with the enormous changes in communications technology over the past 30 years. With the development of new communications over cellular telephones, the Internet, and other technologies that Congress did not anticipate and could not have anticipated back in 1978, the foreign domestic dichotomy that Congress built into the statute has broken down. As a result of that, FISA now covers a wide range of foreign activities that it did not cover back in 1978, and as a result of that, the executive branch and the FISA Court are now required to spend a substantial share of their resources every year to apply for and process court orders for surveillance activities against terror suspects and terrorist associates who are located overseas -- resources that would be far better spent protecting the privacy interests of persons here in the United States.

We believe this problem needs to be fixed, and we submit that we can best fix it by restoring FISA to its original purpose. And to do that, we propose redefining the term "electronic surveillance" in a technology-neutral manner. Rather than focusing, as FISA does today, on how a communication travels or where it is intercepted, we should define FISA's scope by who is the subject of the surveillance, which really is the critical issue for civil liberties purposes. If the surveillance is directed at a person in the United States, FISA generally should apply. If the surveillance is directed at a person outside the United States, it should not.

This would be a simple change, but it would be a critically important one. It would refocus FISA's primary protections right where they belong, which is on persons within the United States.

It would realign FISA and our FISA Court practice with the core purpose of the statute, which is the protection of the privacy interests of Americans inside America. And it would provide the men and women of the intelligence community with the legal clarity and the operational agility that we need to surveil potential terrorists who are overseas. Such a change would be a very significant step forward both for our national security and for our civil liberties.

I want to thank you, all the members of the committee, for your willingness to consider this legislative proposal as well as the other proposals in the package that we submitted to Congress, and I stand ready to answer any questions that you might have.

Thank you.

SEN. ROCKEFELLER: Thank you, sir, very much. We appreciate that.

And as I understand it, Director McConnell, all the other members of the panel are available also to answer questions.

MR. McCONNELL: Yes, sir, that's correct.

SEN. ROCKEFELLER: If I might start, the administration's proposed change to FISA would exempt any international communications in and out of the United States from requiring the review and approval of a FISA judge before the surveillance took place unless a U.S. person was the specific target of the surveillance. In other words, phone calls between foreign targets and Americans located in the U.S. could be intercepted without regard to whether a probable cause standard was demonstrated to the court. This change in law, if enacted, would increase the number of communications involving U.S. persons being intercepted without a court warrant, which would be -- and that would be at unprecedented levels.

So my question, in a sense, is a little bit like what Mr. Wainstein was talking about; that if you're targeting a foreign person -- and I stay within bounds here, but if you're targeting a foreign person, you're also at the same time picking up a United States citizen. You're not just sort of picking up one and not the other. So I'm not sure how that protects the United States citizen, number one. I need to know that.

Secondly, what private safeguards are there in the administration's bill for the communications of Americans who are not a target but whose communications would be otherwise legally intercepted under a bill, which is sort of the same question that I just asked. If the court does not play a role in reviewing the appropriateness of surveillance that may ensnare the international phone calls of Americans, who -- under the administration's proposal -- would oversee those exempt communications to ensure that U.S. persons were not being targeted?

MR. McCONNELL: Sir, I have to --

SEN. ROCKEFELLER: Who watches?

MR. McCONNELL: Let me be careful in how I frame my answer, because I will quickly get into sources and methods that we would not desire those plotting against us, terrorists, to understand or know about.

But in the lead to your statement, where you said a person inside the United States calling out, in all cases that would be subject to a FISA authorization. In the context of intelligence, it would be a foreign power or an agent of foreign power, calling out.

Now, if a known terrorist called in and we're targeting the known terrorist, and someone answers the telephone in the United States, we have to deal with that information.

SEN. ROCKEFELLER: And I understand that and don't disagree with that, in fact support that. But my question is, in the process of carrying that out, properly, because you're -- you have reason to believe, so to speak -- nevertheless the U.S. citizen is being recorded and is a part of the record. And therefore is that person's privacy targeted or not, even if that person is not the purpose of the action?

MR. McCONNELL: The key is "target" and would not be a target of something we were attempting to do. And since FISA was enacted in 1978, we've had the situation to deal with on a regular basis.

Recall in my statement I said in those days most overseas communications were wireless. Americans can be using that overseas communications. So as a matter of due course, if you're targeting something foreign, you could inadvertently intercept an American.

The procedures that were established following FISA in 1978 are called minimize. There is a(n) established rigorous process --

SEN. ROCKEFELLER: I understand.

MR. McCONNELL: And so that was how -- that is how you would protect it.

Let me turn it over to General Alexander, who have a -- more current than I am on specific detail.

LTG KEITH ALEXANDER: Sir, if I might, if you look at where on the network you intercept that call, if we were allowed to intercept that overseas without a warrant, we'd pick up the same call talking to a person in the U.S. In doing that, we have rules upon which we have to abide to minimize the U.S. person's data that's handed down to us from the attorney general. Everyone at NSA is trained on how to do that.

It would apply the same if that were done in the United States under the changes that we have proposed. So we have today a discrepancy on where we collect it.

And the second -- as Director McConnell pointed out, the minimization procedures would be standard throughout the world on how we do it. If a U.S. person was intercepted, if it was overseas or in the States, in both cases we'd minimize it.

SEN. ROCKEFELLER: I will come back to that. My time is up, and I call on the distinguished vice chairman.

SEN. BOND: I thank the distinguished chairman.

And I think that -- Mr. Chairman, that answer is one which we should fully develop in a closed session, because I think that we're -- we -- there's lots more to be said about that. And I think that question would be -- will be a very interesting one to explore later.

I'd ask Admiral McConnell or General Alexander, without getting in any classified measures, can you give us some insight maybe, General, or a specific example how important FISA is to defending ourselves against those who have vowed to conduct terrorist attacks on us?

MR. McCONNELL: Sir, let me start for a general observation, and I want to compare when I left and when I came back. And then I'll turn it to General Alexander for specifics.

The way you've just framed your question -- when I left in 1996, retired, it was not significant. It was almost insignificant. And today it is probably THE most significant ability we have to target and be successful in preventing attacks.

LTG ALEXANDER: Sir, as Director McConnell said, it is the key on the war on terrorism. FISA is the key that helps us get there.

Having said that, there's a lot more that we could and should be doing to help protect and defend the nation.

MR. McCONNELL: Senator, I just might add -- since I'm coming back to speed and learning the issues and so on -- what I'm amazed with is under the construct today, the way the definitions have played out and applied because technology changes, we're actually missing a significant portion of what we should be gathering.

SEN. BOND: I think probably we want to get into that later, but I would, I guess, in summary, you would say that this -- you said this is the most important tool, and the information that you've gained there has allowed us on a number of occasions to disrupt activities that would be very harmful abroad and here.

Is that a fair statement?

MR. McCONNELL: Inside and outside the United States.

SEN. BOND: All right. Mr. Wainstein, the proposal includes a new definition for an agent of a foreign power who possesses foreign intelligence information.

Can you give us an example of the type of person this provision is intended to target, and how that meets the particularity and reasonableness requirement of the Fourth Amendment?

MR. WAINSTEIN: Thank you, Senator. Speaking within the parameters of what we can talk about here in open session -- and I think that's a particular concern in this particular case, where identifying any example with great particularity could actually really tip off our adversaries.

Let me just sort of keep in general terms, that this new definition of an agent of foreign power would fill a gap in our coverage right now, which is that there are situations where a person, a non-U.S. person -- this is only non-U.S. person -- is here in the United States. That person possesses significant foreign intelligence information that we would want to get that could relate to the intent of foreign powers who might want to do us harm. But because we cannot connect that person to a particular foreign power -- under the current formulation of agent of foreign power, we're not able to go to the FISA Court and get approval, get an order allowing us to surveil that person.

So, you know, keep in mind, this is a FISA Court order. We'd do this pursuant to the FISA Court's approval. This is intended to provide that -- fill that gap, similar to what Congress did when it gave us the lone wolf provision a couple years ago, allowing us to target some terrorists whom we could not connect to a particular foreign power.

That's critically important, and I would ask if I could defer to a closed session --

SEN. BOND: We'll finish that up.

Another broader question. The recent inspector general's report detailed too many errors in the FBI's accounting for and issuing national security letters. As a result, there -- some have suggested that the national security letter authorities should be changed or limited. What impact would changing the standard from -- relevance to a higher standard have on FBI operations, particularly in obtaining FISA surveillance and search authorities?

MR. WAINSTEIN: Well, the --

SEN. BOND: Or is that Mr. Powell -- is that Mr. Wainstein or Mr. Powell --

MR. BENJAMIN POWELL: I don't know what numbers what would be cut out if the standard were changed. I think it is important to note -- and this committee has available to it the classified inspector general report that goes into great detail of where NSLs have been used in specific cases to obtain very critical information to enable foreign intelligence investigations to go forward, so I think if the standard were changed, that would lead to a real impact on those investigations. But Mr. Wainstein is closer to those and may want to comment.

MR. WAINSTEIN: I'll just -- I'll echo what Mr. Powell said. And I believe that the remedy or the way of addressing the failings -- which were failings; it's been acknowledged as serious failings by the director of the FBI and the attorney general -- is not to scale back on the authority but to make sure that that authority is well-applied. And there are many things in process right now to make sure that'll happen.

SEN. BOND: Just follow the rules.

Thank you very much, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Vice Chairman Bond.

Senator Wyden.

SEN. RON WYDEN (D-OR): Thank you, Mr. Chairman.

Admiral, I very much appreciated our private conversations and discussion about how we balance this efforts in terms of fighting terrorism ferociously and protecting privacy. And what I want to examine with you is, what's really going to change on the privacy side?

For example, in the debate about national security letters, when Congress expanded the authority to issue these letters to thousands of Americans, most of the very same terms were used then that have been used this afternoon, efforts, for example, such as minimizing the consequences of the law. But recently the director of the FBI has admitted that there was widespread abuse of the national security letter authority, that there were instances when agents claimed emergency powers despite the lack of an actual emergency.

What is going to change now with this new effort, so that we don't have administration officials coming, as the attorney general recently did, to say, made a mistake -- widespread abuse?

MR. McCONNELL: First of all, the proposal is privacy-neutral. It doesn't change anything. NSLs are not a part of FISA.

SEN. WYDEN: I understand that. But what concerns me, Admiral, is, we were told exactly the same thing with national security letters. We asked the same questions. We were told that there would be efforts to minimize the consequences. And I want to know, what's going to be different now than when we were told there wouldn't be abuses in the national security letters?

MR. McCONNELL: Sir, let me separate the two, if I could, to comment on -- FISA grew out of abuses that occurred in the '70s, as I mentioned in my opening statement. As a result of that, the hearings that were held by this body with regard to how we administer it going forward, the intelligence community was given very strict guidance with regard to the law and the implementing instructions and so on. There are instructions, and I think if you check back in time, the signature on the -- the instruction that NSA lives by still has my name on it. It's called USID (sp) 18.

Now what I'm setting up for you is a community whose job is surveillance, whose very existence is for surveillance, and that community was taught daily, regularly, signed a note each year, retrained. And we focused on it in a way to carry out exactly the specifics of law. Let me contrast that with the FBI. FBI has a new mission. It's a new focus. And think of it as the -- in the previous time as, arrest and convict criminals. Now it's to protect against terrorism, so it's a new culture adopting to a new set of authorities.

Now they were admitted by the director of FBI and the attorney general. Mistakes were made and they're cleaning that up. But it was done in a time when it was different in change, and that culture is evolving to do it --

SEN. WYDEN: So you're saying that those who will handle the new FISA statute are more expert and will want to inquire in secret session about that.

Now another section of the bill would grant immunity from liability to any person who provided support to the warrantless wiretapping program or similar activities. Would this immunity apply even to those who knowingly broke the law?

MR. McCONNELL: Of course not, Senator. It would never apply to anybody who knowingly broke the law.

SEN. WYDEN: How is the bill going to distinguish between intentional lawbreakers from unintentional lawbreakers? One of the things that I've been trying to sort out, and we've -- strange discussion about some of the classified materials -- is, how are you going to make these distinctions? I mean, if we find out later that some government official did knowingly break the law in order to support the warrantless wiretapping program, could that then be used to grant them immunity? We need some way to make these distinctions.

MR. McCONNELL: Well, first of all, Senator, you're using the phrase "warrantless surveillance." Part of the objective in this proposal is to put all of the surveillance under appropriate authority, to include warrants where appropriate. Now if someone has violated the law, and it's a violation of the law, there could be no immunity.

SEN. WYDEN: In January of this year, Attorney General Gonzales wrote to the Judiciary Committee and stated that any electronic surveillance that was being committed as part of the warrantless wiretapping program would, and I quote, "now be conducted subject to the approval of the Foreign Intelligence Surveillance Court."

Does this mean that the federal government is now obtaining warrants before listening to Americans' phone calls?

MR. McCONNELL: Sir, the way you're framing your question, as if the intent was to listen to Americans' phone calls, that's totally incorrect. The --

SEN. WYDEN: Well, simply --

MR. McCONNELL: The purpose is to listen to foreign phone calls. Foreign. Foreign intelligence. That's the purpose of the whole -- think of the name of the act: Foreign Intelligence Surveillance Act -- not domestic, not U.S.

SEN. WYDEN: But is the federal government getting warrants?

MR. McCONNELL: For?

SEN. WYDEN: Before it's listening to a call that involves Americans?

MR. McCONNELL: If there is a U.S. person, meaning foreigner in the United States, a warrant is required, yes.

SEN. WYDEN: The government is now, then, completely complying with the warrant requirement?

MR. McCONNELL: That is correct.

SEN. WYDEN: Okay.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Wyden.

And we now go to Senator Feingold.

SEN. RUSSELL FEINGOLD (D-WI): Thank you very much, Mr. Chairman, for holding this hearing. And I have a longer statement I'd like to place in the record. And I'd ask the chairman if I could do that.

SEN. ROCKEFELLER: Without objection.

SEN. FEINGOLD: I thank the witnesses for testifying today.   Can each of you assure the American people that there is not -- and this relates to what -- the subject Senator Wyden was just discussing -- that there is not and will not be any more surveillance in which the FISA process is sidestepped based on arguments that the president has independent authority under Article II or the authorization of the use of military force?

MR. McCONNELL: Sir, the president's authority under Article II is -- are in the Constitution. So if the president chose to exercise Article II authority, that would be the president's call.

What we're attempting to do here with this legislation is to put the process under appropriate law so that it's conducted appropriately to do two things -- protect privacy of Americans on one hand, and conduct foreign surveillance on the other.

SEN. FEINGOLD: My understanding of your answer to Senator Wyden's last question was that there is no such activity going on at this point. In other words, whatever is happening is being done within the context of the FISA statute.

MR. McCONNELL: That's correct.

SEN. FEINGOLD: Are there any plans to do any surveillance independent of the FISA statute relating to this subject?

MR. McCONNELL: None that -- none that we are formulating or thinking about currently.

But I'd just highlight, Article II is Article II, so in a different circumstance, I can't speak for the president what he might decide.

SEN. FEINGOLD: Well, Mr. Director, Article II is Article II, and that's all it is.

In the past you have spoken eloquently about the need for openness with the American people about the laws that govern intelligence activity. Just last summer, you spoke about what you saw as the role of the United States stating that, quote, "Because of who we are and where we came from and how we lived by law," unquote, it was necessary to regain, quote, "the moral high ground."

Can you understand why the American people might question the value of new statutory authorities when you can't reassure them that you consider current law to be binding? And here, of course, you sound like you're disagreeing with my fundamental assumption, which is that Article II does not allow an independent program outside of the FISA statute, as long as the FISA statute continues to read as it does now that it is the exclusive authority for this kind of activity.

MR. McCONNELL: Sir, I made those statements because I believe those statements with regard to moral high ground, and so on. I live by them.

And what I'm attempting to do today is to explain what it is that is necessary for us to accomplish to be able to conduct the appropriate surveillance to make -- to protect the American people, consistent with the law.

SEN. FEINGOLD: Let me ask the other two gentlemen.

General Alexander, on this point with regard to Article II, I've been told that there are no plans to take warrantless wiretapping in this context, but I don't feel reassured that that couldn't reemerge.

LTG ALEXANDER: Well, I agree with the way Director McConnell laid it out.

I would also point out two things, sir. The program is completely auditable and transparent to you so that you and the others -- and Senator Rockefeller, I was remiss in (not) saying to you and Senator Bonn thank you for statements about NSA. They are truly appreciated.

Sir, that program is auditable and transparent to you so that you as the oversight can see what we're doing. We need that transparency and we are collectively moving forward to ensure you get that. And I think that's the right thing for the country.

But we can't change the Constitution. We're doing right now everything that Director McConnell said is exactly correct for us to.

SEN. FEINGOLD: Well, here's the problem. If we're going to pass this statute, whether it's a good idea or a bad idea, it sounds like it won't be the only basis on which the administration thinks it can operate. So in other words, if they don't like what we come up with, they can just go back to Article II. That obviously troubles me.

Mr. Wainstein?

MR. WAINSTEIN: Well, Senator, as the other witnesses have pointed out, the Article II authority exists independent of this legislation and independent of the FISA statute. But to answer your question, the surveillance that was conducted, as the attorney general announced, that was conducted pursuant to the president's terrorist surveillance program, is now under FISA Court order.

SEN. FEINGOLD: Another topic. It would be highly irresponsible to legislate without an understanding of how the FISA Court has interpreted the existing statute. Mr. Wainstein, will the Department of Justice immediately provide the committee with all legal interpretations of the FISA statute by the FISA Court along with the accompanying pleadings?

MR. WAINSTEIN: I'm sorry, Senator; all FISA Court interpretations of the statute?

SEN. FEINGOLD: All legal interpretations of the FISA statute by the FISA Court, along with the accompanying pleadings.

MR. WAINSTEIN: In relation to all FISA Court orders ever --

SEN. FEINGOLD: In relation to relevant orders to this statutory activity.

MR. WAINSTEIN: Well, I'll take that request back, Senator. That's the first time I've heard that particular request, but I'll take it back.

SEN. FEINGOLD: Well, I'm pleased to hear that, because I don't see how the Congress can begin to amend the FISA statute if it doesn't have a complete understanding of how the statute has been interpreted and how it's being currently used. I don't know how you legislate that way. MR. WAINSTEIN: Well, I understand, but obviously, every time they issue an order, that is -- that can be an interpretation of how the FISA statute is -- interpretation of the FISA statute. And as you know from the numbers that we issue, we have a couple thousand FISAs a year. So that would be quite a few documents.

SEN. FEINGOLD: This is an important matter. If that's the number of items we need to look at, that's the number we will look at.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Feingold.

Senator Nelson.

SEN. BILL NELSON (D-FL): Mr. Chairman, most of my questions I'm going to save for the closed session, but I would like to ascertain the administration's state of mind with regard to the current law. In the case where there is a foreign national in a foreign land calling into the United States, if you do not know the recipient's nationality and therefore it is possible it is a U.S. citizen, do you have to, in your interpretation of the current law, go and get a FISA order?

MR. McCONNELL: No, sir, not if it -- if the target is in a foreign country and our objective is to collect against the foreign target, and they call into the United States, currently it would not require a FISA. And let me double-check that. I may be -- I'm dated.

LTG ALEXANDER: If it's collected in the United States, it would require a FISA if we do not know who the end is to, or under the program it would have to be collected. If it were known, both ends foreign, known a priori, which is hard to do in this case, you would not. If it was collected overseas, you would not.

SEN. BILL NELSON: Let's go back to your second -- General, your second answer.

LTG ALEXANDER: If you know both ends -- where the call is going to go to before he makes the call, then you know that both ends were foreign; if you knew that ahead of time, you would not need a warrant.

SEN. NELSON: If you knew that.

LTG ALEXANDER: If you knew that.

SEN. NELSON: If you did not know that the recipient of the call in the U.S. is foreign, then you would have to have a FISA order.

LTG ALEXANDER: If you collected it in the United States. If you collected it overseas, you would not.

SEN. NELSON: Well, since in digital communications, if these things -- little packets of information are going all over the globe, you might be collecting it outside the United States, you might be collecting it inside the United States.

MR. McCONNELL: And Senator, that's our dilemma. In the time in 1978 when it was passed, almost everything in the United States was wire, and it was called electronic surveillance. Everything external in the United States was in the air, and it was called communications intelligence.

So what changed is now things in the United States are in the air, and things outside are on wire. That's the --

SEN. NELSON: I understand that, but -- now, I got two different answers to the same question from you, Mr. Director, and from you, General.

MR. McCONNELL: It depends on where the target is and where you collect it. That's why you heard different answers.

SEN. NELSON: So if you're collecting the information in the United States --

MR. McCONNELL: It requires a FISA.

SEN. NELSON: Okay. Under the current law, the president is allowed 72 hours in which he can go ahead and collect information and, after the fact, go back and get the FISA order.

Why was that suspended before in the collection of information?

LTG ALEXANDER: Sir, I think that would best be answered in closed session to give you exactly the correct answer, and I think I can do that.

SEN. NELSON: And -- well, then, you can acknowledge here that is -- it was in fact suspended.

SEN. ROCKEFELLER: I would hope that that would be -- we would leave this where it is.

SEN. NELSON: All right. I'll just stop there.

SEN. ROCKEFELLER: Thank you, Senator Nelson.

Senator Feinstein.

SEN. DIANNE FEINSTEIN (D-CA): Thank you very much, Mr. Chairman. The administration's proposal, Admiral, doesn't address the authority that the president and attorney general have claimed in conducting electronic surveillance outside of FISA. While the FISA Court issued a ruling that authorized the surveillance ongoing under the so-called TSP, Terrorist Surveillance Program, the White House has never acknowledged that it needs court approval. In fact, the president, under this reasoning, could restart the TSP tomorrow without court supervision if he so desired.

Now, Senator Specter and I have introduced legislation which very clearly establishes that FISA is the exclusive authority for conducting intelligence in the United States.

Here's the question: Does the administration still believe that it has the inherent authority to conduct electronic surveillance of the type done under the TSP without a warrant?

MR. McCONNELL: Ma'am, the effort to modernize would prevent an operational necessity to do it a different way. So let me -- I'm trying to choose my words carefully.

SEN. FEINSTEIN: Yes, but my question is very specific. Does the president still believe he has the inherent authority to wiretap outside of FISA? It's really a yes or no question.

MR. McCONNELL: No, ma'am, it's not a yes or no question.

SEN. FEINSTEIN: Oh --

MR. McCONNELL: Sorry -- I'm sorry to differ with you. But if you're asking me if the president is abrogating his Article II responsibilities, the answer is no. What we're trying to frame is -- there was an operational necessary for TSP that existed in a critical period in our history, and he chose to exercise that through his Article II responsibility.

We're now on the other side of that crisis, and we're attempting to put it consistent with law, so it's appropriately managed and subjected to the appropriate oversight.

SEN. FEINSTEIN: Well, the way I read the bill, very specifically, the president reserves his authority to operate outside of FISA. That's how I read this bill. I think that's the defining point of this bill.

Not only that; in Section 402, Section 102(a), notwithstanding any other law, the president, acting through the attorney general, may authorize electronic surveillance without a court order under this title, to inquire (sic) foreign intelligence information for periods of up to one year. And then it goes on to say if the attorney general does certain things.

MR. McCONNELL: Yeah.

SEN. FEINSTEIN: I mean, clearly this carves out another space. That's the question.

MR. McCONNELL: That same situation existed in 1978, when the original FISA law was passed. What we're attempting to balance is emergency response to a threat to the nation, consistent with our values and our laws. So the way this operated for 30 years, almost 30 years -- we operated day to day, and it was appropriately managed and appropriate oversight. We had a crisis. The president responded to the crisis, and we're now attempting to accommodate new threats that we didn't understand in 2002, to be able to respond to protect the nation, to protect the nation and its citizens today, consistent with the appropriate oversight.

Does that mean the president would not exercise Article II in a crisis? I don't think that's true. I think he would use his Title II responsibilities -- (inaudible) -- Article II.

MR. POWELL: And Senator, if I may add, Section 402 is not meant to carve out in any way or speak to what the scope of the president's power is. That is meant to speak to Title III and criminal warrants and making clear what the certification procedure was. I was a part of this working group for over a year and a half, and the decision was specifically taken not to speak to, one way or the other, the scope of the president's constitutional power under Article II or to address this -- that in this proposal in any way, whether to expand it or contract it; it was simply meant to be silent on what the president's Article II powers are.

I would also note, in the idea that the president can sidestep FISA or use Article II authority to simply place the statute aside, that is not my understanding of the Department of Justice position or the president's position. When you look at the legal analysis that has been released by the Department of Justice on the Terrorist Surveillance Program, that speaks to a very limited set, speaking to al Qaeda and its affiliates, in which we are placed in a state of armed conflict with, and speaking to the authorization of the use of military force passed by the -- by this Congress.

It does not speak to any kind of broad Article II authority of the president to simply decide to set FISA aside in toto and conduct electronic surveillance in a broad manner, unconnected to things like the authorization for the use of military force or the state of armed conflict that we entered into with al Qaeda.

So I have not seen anything from the Department of Justice or the president that would suggest that he would simply set aside FISA or has the authority to simply conduct electronic surveillance under Article II essentially unconnected to events in the world.

SEN. FEINSTEIN: I can see that my time is up. But there is nothing in this bill which reinforces the exclusive authority of FISA? There is nothing in this bill that confines the president to work within FISA?

MR. POWELL: This bill does nothing to change what FISA currently says, which is electronic surveillance shall be -- FISA shall be the exclusive means for conducting electronic surveillance unless otherwise authorized by statute. This bill simply leaves that statement as is. It does not strike it, it does not change it. It leaves it unchanged.

SEN. FEINSTEIN: My time is up, but this is a good issue to pursue.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Feinstein.

Senator Whitehouse.

SEN. SHELDON WHITEHOUSE (D-RI): Thank you, Chairman.

We'll talk more about this obviously in the closed session, but I wanted to make a couple of points. And before I do, Director, let me say that I'm going to be speaking rather generally. As between you and I, I believe you to be an honorable and trustworthy man. I think that you are here with a view to be professional; that is your motivation. You are not an ideologue or a partisan in your desire to help prepare the intelligence function of the United States, and I applaud you for that.

But that said, you are still asking for substantial changes in your authority. And as an aside, I think the new technologies that have emerged do suggest some adjustment to FISA. It may be over or underinclusive in certain areas. But as we look through the lens of the past in terms of evaluating how much we can trust you with institutionally -- you know, these are tough times. As you said, we had FISA -- the reason we have FISA in the first place is because of past abuses. We've just found out about the litany of national security letter abuses within the Department of Justice. The attorney general has thoroughly and utterly lost my confidence, and at this stage, any element of the FISA legislation that depends on the attorney general will need some other backstop in order to have my confidence.

We are coming out of this Article II regime of the TSP Program of warrantless wiretapping, and to this day, we have never been provided the presidential authorization that cleared that program to go or the attorney general-Department of Justice opinions that declared it to be lawful.

Now, if this program is truly concluded, the TSP program, and if this is the new day in which everything is truly going to be under FISA, I can't imagine for the life of me why those documents that pertain to a past and closed program should not be made available to the committee and to us. And so, to me, it's very concerning as we take these next steps for you to be saying impliedly, "Trust us, we need this authority, we'll use it well," when we're coming off the record of the national security letters; we're coming off terrible damage done to the Department of Justice by this attorney general; we're coming off a continuing stone-wall from the White House on documents that I cannot for the life of me imagine merit confidentiality at this stage.

And in the context of all of that -- you got some up-hill sledding with me, and I want to work with you and I want to do this, but it would be a big step in the right direction, in terms of building the trust. Mr. Powell, I heard you just talk about how important it was that to the extent we've been disclosed, these opinions, that there was not transparency. We've been talking a lot about transparency and all that kind of stuff.

Where's the transparency as to the presidential authorizations for this closed program? Where is the transparency as to the attorney general opinions as to this closed program? That's a pretty big "We're not going to tell you" in this new atmosphere of trust we're trying to build.

If you have a response, sir, you'd like to make to that --

MR. McCONNELL: I do, sir.

SEN. WHITEHOUSE: -- I'd be delighted to hear it. I know it was not framed as a question.

MR. McCONNELL: I do have a response. I think the appropriate processes were created as a result of abuses of the `70s. They were inappropriate. We've got oversight committees in both the Senate and the House. We're subjected to the appropriate oversight, rigorous, as it should be. Laws were passed to govern our activities. Those were inspected. We have inspector's general, and the process has worked well.

I've made a recommendation based on just coming back to the administration with what we should do with regard to disclosing additional information to this committee, and that recommendation is being considered as we speak. Certainly, it's easier for me to share that information with you and to have a dialogue about what is said, and how it worked, and did it work well, and should we change it.

But until I get working through the process, I don't have an answer for you yet. But oversight is the appropriate way to conduct our activities going forward consistent with the law.

SEN. WHITEHOUSE: It's wonderful to hear you say that.

MR. WAINSTEIN: If I may, Senator -- may I just respond to that very briefly, Mr. Chairman?

SEN. WHITEHOUSE: Please.

MR. WAINSTEIN: Senator, to the extent that you've voiced some concern about lack of confidence in the Department of Justice and our role in FISA --

SEN. WHITEHOUSE: No. Just to be clear -- lack of confidence in the attorney general.

MR. WAINSTEIN: Well, if I may just say that I'm the head of a brand-new division that's focused on national security matters, and a large part of our operation is making sure that we play within the lines. We got a lot of people dedicated to that, and I can tell you that our deputy attorney general and our attorney general are very conscientious about handling all FISA matters, get reported to regularly, handle -- their responsibilities are to sign off on those packages very carefully and conscientiously.

And as far as the NSL matter goes, both the director of the FBI and the attorney general were quite concerned about that and have put in place a very strong set of measures to respond to it. So I think if you look at their response to that problem, which was a very serious problem, I would hope that that would give you some more confidence.

SEN. WHITEHOUSE: Thanks.

SEN. ROCKEFELLER: Thank you, Senator Whitehouse.

Senator Snowe.

SEN. OLYMPIA J. SNOWE (R-ME): Thank you, Mr. Chairman.

Director McConnell, obviously this is creating this delicate balance. And I know in your testimony, you indicated, as we redefine the electronic surveillance and obviously amend the Foreign Intelligence Surveillance Act, that to provide the greater, you know, flexibility in terms of communication, that we don't upset the delicate balance with respect to privacy questions.

Last September, Kate Martin, the director of the Center for National Security Studies, testified before the Crime, Terrorism and Homeland Security Subcommittee of the House Judiciary Committee and indicated that this bill would radically amend the FISA Act and eliminate the basic framework of the statute and create such large loopholes in the current warrant requirement that judicial warrants for secret surveillance of Americans' conversations and e-mails would be the exception rather than the rule. How would you respond to such a characterization? And could you also explain to the committee how exactly the framework has been preserved through this renewed version of FISA?

MR. McCONNELL: Well, first of all, I characterize the statements you just read as uninformed, because the way it was framed -- it's as if we were targeting without any justification communications of U.S. citizens, which is not the case, simply not the case. If there is a reason to target any communications and it's inside the United States, it would require a FISA warrant in the current law and in the future law.

So the only thing we're doing with the bill, the proposal, is just to update it to make it technology neutral. All things regarding privacy stay the same.

SEN. SNOWE: And so there's no -- in your estimation, then, there aren't any provisions in this proposal that would create such large loopholes.

MR. McCONNELL: Indeed not. No.

SEN. SNOWE: No deviation, other than to make it technology neutral.

MR. McCONNELL: Zero. None.

SEN. SNOWE: I noted in your statement that you mentioned additional protections besides obviously, submitting -- coming before the respective intelligence committees and also to the leadership regarding the Privacy and Civil Liberties Oversight Board that was established by the legislation that created the department in 2004. Exactly what has that board accomplished to this date? As I understand, it was just constituted last year in terms of all the appointments being completed. So exactly what has this board done in the interim that would suggest that they will provide additional oversight?

MR. McCONNELL: I've only met them recently and engaged with them and we have a regular cycle for meeting and discussing their activities, but it is oversight of the process to look at activities, to see what's being conducted, and they have a responsibility to report on it to the president and to others of us. They work in my organization to carry out their duties, which is to ensure that all of our activities are consistent with civil liberties and the appropriate protection of privacy.

MR. POWELL: Senator, there’s also –- they've just released their first report. It's a detailed report, talks about the numbers of programs that they have reviewed, including an in-depth review of what was formerly the terrorist surveillance program before being placed under FISA. I think you'll find that report informative about what their findings were about the program. They've done some in- depth reviews of various programs both inside and outside the intelligence community, including they've attended NSA's training that is provided to its operators, and that is a public report.

Vito, I don't know if you want -- you've interacted with them more. They've spent a lot of time in different programs across this government, and that report lays it out, and it's up on the Web.

MR. VITO POTENZA: No, Senator, there's not much more to add to that. They did come out to NSA. They -- as Mr. Powell said, they sat in on training, they reviewed the -- specifically the Terrorist Surveillance

Program. They came out at least twice and spent a considerable amount of time with us.

SEN. SNOWE: And when were they fully constituted as a board?

MR. McCONNELL: We have the head of the board here in the audience somewhere. Let me -- get him to -- he was here. Still with us?

Senator, I'll get back to you on it. I don't know the exact time, but we'll provide it to you.

SEN. SNOWE: And certainly would they be giving I think reasonable assurances to the American people that they will be overseeing and protecting their privacy --

MR. McCONNELL: That's their purpose.

SEN. SNOWE: -- consistent with the law?

MR. McCONNELL: That is their purpose, and as just mentioned, the first report is posted on the website. I didn't know it was actually already on the website.

SEN. SNOWE: Thank you.

SEN. ROCKEFELLER: Thank you, Senator Snowe.

Senator Levin.

SEN. CARL LEVIN (D-MI): Thank you, Mr. Chairman.

The FISA Court interpreted -- or issued some orders in January. These are the orders which were the subject of some discussion here today. Do we have copies of all those orders, the January orders of the FISA Court?

MR. WAINSTEIN: Yes. And the -- all members of the committee I think have been briefed in on them or --

SEN. LEVIN: But do we have copies of the orders?

MR. WAINSTEIN: I believe you all have copies, yes.

SEN. LEVIN: How many are there?

MR. WAINSTEIN: How many copies?

SEN. LEVIN: How many orders?

MR. WAINSTEIN: I cannot get into how many orders there are.

SEN. LEVIN: You can't get into the number?

MR. WAINSTEIN: Not in open session.

SEN. LEVIN: Into the number of orders?

MR. WAINSTEIN: Yeah, not in open session, Senator.

SEN. LEVIN: Okay. Have those orders been followed?

MR. WAINSTEIN: Yes, sir.

SEN. LEVIN: And have you been able to carry out the new approach that those orders laid out so far?

MR. WAINSTEIN: I'd prefer to, if we could, defer any questions about the operation of the orders to closed session.

SEN. LEVIN: No, I'm not getting into the operations. I want to know, have you been able to implement those orders?

MR. WAINSTEIN: We have followed the orders, yes, sir.

SEN. LEVIN: Without any amendments to the statute?

MR. WAINSTEIN: There have been no amendments to the statute since the orders were signed in January.

SEN. LEVIN: And you've been able to follow the new orders without our amending the statute?

MR. WAINSTEIN: We have --

LTG ALEXANDER: Sir, could I answer?

SEN. LEVIN: Just kind of briefly, I mean let me ask the question a different ways. Are the orders dependent upon our amending the statute?

LTG ALEXANDER: No, the current orders are not.

SEN. LEVIN: Okay.

LTG ALEXANDER: Nor are the current orders sufficient for us to do what you need us to do.

SEN. LEVIN: I understand that. But in terms of the orders being implementable, they do not depend upon our amending the statute.

Is that correct?

LTG ALEXANDER: That's correct. The current state that we're in does not require that.

SEN. LEVIN: Good.

LTG ALEXANDER: But I would also say, that's not satisfactory to where you want us to be.

MR. McCONNELL: Senator, what you need to capture is, we were missing things that --

SEN. LEVIN: I understand. I understand that we're not deterring the implementation of the orders.

Now the -- back in January, the -- there was an article that says that the administration continues to maintain that it is free to operate without court approval. There seemed to be some question about that here today. Is that not the administration's position?

MR. McCONNELL: That is not the administration's position that I understand, sir.

SEN. LEVIN: Okay.

Back in January on the 17th, the attorney general wrote to Senators Leahy and Specter the following, that a judge of the Foreign Intelligence Surveillance Court issued orders authorizing the government to target for collection international communications into or out of the United States, where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization. Has that remained the test for when you want to be able to target a communication that is -- where the target is in the United States? Is that, there must be probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization?

MR. POWELL: Senator, I think it would be best if we get into that in closed session.

SEN. LEVIN: Well, is there any change in that? This to me is the key issue, the probable cause issue --

MR. POWELL: Senator, you have copies of those orders that lay out very specifically what those tests are. What the attorney general's letter did was speak to what the president had laid out in his December 17th, 2005 radio address as the Terrorist Surveillance Program.

SEN. LEVIN: I understand.

MR. POWELL: And that is what that letter is addressed to, Senator --

SEN. LEVIN: My question is, is there any change, that that is what you are limiting yourselves to, situations where, if the target is in the -- if the eavesdropping takes place in the United States, that there must be probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization? Is there any change from that? This is what the attorney general wrote us. Is there any change from that since January 17th?

LTG ALEXANDER: Sir, we can't answer that in open session.

SEN. LEVIN: Well, he wrote it in open session. It's an open letter.

SEN. BOND: Mr. Chairman, I would suggest to the chairman that this question we can explore fully in the closed session.

SEN. LEVIN: Well --

SEN. ROCKEFELLER: I would leave that --

SEN. LEVIN: This is a letter --

(Cross talk.)

SEN. ROCKEFELLER: If that presents a problem say so --

MR. McCONNELL: It presents a problem for us, sir.

SEN. ROCKEFELLER: It is not --

MR. McCONNELL: It presents a problem for us. The way it was framed and the way it was written at the time is absolutely correct. That -- and the way the senator's framing his question that -- it pushes it over the edge for how we can respond to it, because there's been some additional information.

SEN. LEVIN: Could the attorney general write that letter today?

MR. McCONNELL: We can discuss it in closed session, sir.

MR. POWELL: Senator, the point of the attorney general's letter, as I understood it, was to address those things that the president -- had been discussed, that were being done under the Terrorist Surveillance Program. And what his letter addresses is to say that those things that the president had discussed under the program were now being done under orders of the FISA court. And today, as we sit here, the attorney general's letter remains the same: that those things that the president had discussed are -- continue to be done under the orders of the FISA court. So to that extent, there's no change to the attorney general's letter.

LTG ALEXANDER: Sir, if I could, to just clarify this one step further, there are other things that the FISA court authorizes day in and day out that may be included in that order, that go beyond what the attorney general has written there. Every day we have new FISA applications submitted.

MR. McCONNELL: What you were tying this to, Senator, was al Qaeda.

SEN. LEVIN: Mr. Chairman, I think what -- if the chair and vice chair are willing, I think we ought to ask the attorney general then if this letter still stands. In terms of the test which is being applied for these targeted communications, it's a very critical issue. The president of the United States made a representation to the people of the United States as to what these intercepts were limited to. And the question is, is that still true? And it's a very simple, direct question, and we ought to ask the attorney general, since he wrote, made a representation in public; the president has made a representation in public. If that's no longer true, we ought to know it. If it is still true, we ought to know it. So I would ask the chairman and vice --

SEN. ROCKEFELLER: The senator is correct, and that will happen and that will be discussed in the closed session.

SEN. LEVIN: Thank you. My time is up. Thank you.

SEN. ROCKEFELLER: No, thank you, Senator Levin. I'm -- after Vice Chairman Bond has asked his question, I'm yielding my time to the senator from Florida, and I guess then to the senator from Oregon, and then eventually I'll get to ask a question, too.

Senator Bond.

SEN. BOND: Thank you, Mr. Chairman. I think maybe to clear up some of the confusion -- and some of the questions couldn't be answered -- it's my understanding you're before us today asking for FISA updates to enable NSA to obtain under that statute vital intelligence that NSA is currently missing.

And secondly, when we talk about Article II and the power of the president under Article II, presidents from George Washington to George Bush have intercepted communications to determine the plans and intentions of the enemy under the Foreign Intelligence Surveillance authority in that. And prior to the TSP, as I understand it, the most recent example was when the Clinton administration used Article II to authorize a warrantless physical search in the Aldrich Ames espionage investigation.

The Supreme Court in the Keith case in `72 said that the warrant requirement of the Fourth Amendment applies to domestic security surveillance, but it specifically refused to address whether the rule applied with respect to activities of foreign powers or their agents. And then in the Truong case in 1980, the Fourth Circuit noted the constitutional responsibility of the president for the conduct of the foreign policy of the United States in times of war and peace in the context of warrantless electronic surveillance. And it did say that it limited the president's power with a primary purpose test and the requirement that the object be -- the search be a foreign power, its agent or collaborator.

Finally, despite Congress' attempts to make FISA the exclusive means of conducting electronic surveillance for national security purposes, my recollection from law school is that the Constitution is the supreme law of the land. It is a law.

Congress cannot change that law in the Constitution without amending the Constitution. And the Foreign Intelligence Court of Review, in In re Sealed Case, in 2002, Judge Silverman wrote, "We take for granted that the president does have the authority" -- that's the authority to issue warrantless surveillance orders -- "and assuming that is so, FISA could not encroach on the president's constitutional power. We should remember that Congress has absolutely no power or authority or means of intercepting communications of foreign enemies. But -- so even at his lowest ebb, the president still exercises sufficient significant constitutional authority to engage in warrantless surveillance of our enemies."

And I know that there are two admitted lawyers on the panel. Are you a lawyer also? Three. Is that right? Is that correct? Mr. Powell, Mr. Wainstein, Mr. Potenza? Thank you.

SEN. ROCKEFELLER: Just for the record, they nodded "yes." (Laughter.)

SEN. BOND: But we didn't want to disclose all the lawyers on there. I have that problem myself.

I wanted to ask, since we're asking kind of unrelated questions, Mr. Wainstein, the 9/11 commission and this committee tried to get a look at all the intelligence and the policy decisions leading up to 9/11. And I'm beginning to hear that we did not -- maybe the 9/11 commission did not get all the information.

For example, in the case of Mr. Sandy Berger, he admitted removing five copies of the same classified document from the National Archives; destroyed three copies. We know that he was there on two other occasions; we don't know whether he removed other original documents. He removed classified notes without authorization. What we don't know is what was actually in the PDBs that were stuffed in his BVDs. In his plea agreement, he agreed to take a polygraph at the request of the government, and for some reason, the Department of Justice has not gotten around to polygraphing him to ascertain what was in the documents and why he removed them.

Are you going to try to find out that information, and when can you let us know, Mr. Wainstein?

MR. WAINSTEIN: Senator Bond, I know that that is an area of inquiry from other members of Congress, and there's been a good bit of traffic back and forth on that particular issue. I have to admit that right now I'm not up on exactly where that is. So if it's okay with you, I will submit a response in writing.

SEN. BOND: We'd like to find out.

Thank you, Mr. Chairman.

MR. WAINSTEIN: Thank you, sir.

SEN. ROCKEFELLER: Thank you, Mr. Vice Chairman.

And now Senator Nelson, to be followed by Senator Wyden, to be followed by myself.

SEN. BILL NELSON (D-FL): Thank you, Mr. Chairman.

I want to go back to the line of questioning before. You already said that under current law, if there is someone who is deemed to be of interest outside of the United States that's calling in, even though we may not know that the person in the United States is a U.S. citizen, that that -- under current law, that would require a FISA order?

MR. McCONNELL: Depends on where the intercept takes place.

SEN. NELSON: Okay. And so if the intercept takes place in the United States --

MR. McCONNELL: It requires an order.

SEN. NELSON: Okay. Now --

MR. POTENZA: Senator, if I may, I would just add to that -- if it's on a wire in the United States, it requires a FISA order.

SEN. NELSON: So if it's a cell phone, it doesn't require -- if it --

MR. POTENZA: A separate section of FISA would cover that. But the particular situation you were talking about is the wire section.

MR. McCONNELL: In '78, they separated it between "wire" and "wireless." And so if a wireless call was made from overseas into the United States via satellite, it's -- would be available for collection.

SEN. NELSON: Right. Is it the case under current law where all parties to a communication are reasonably believed to be in the United States, that the government would need to go to a FISA court to obtain an order authorizing the collection?

MR. McCONNELL: Yes, sir, that's correct.

SEN. NELSON: Under your new proposal, is that the case?

MR. McCONNELL: That's correct. Yes, sir, it is correct.

SEN. NELSON: The proposed definition of electronic surveillance depends on whether a person is reasonably believed to be in the United States. What kind, Mr. Wainstein, of guidance would the Justice Department give when someone is reasonably believed to be in the United States?

MR. WAINSTEIN: Sir, I can't give you specific indicia that we would use. We might be able to elaborate more in closed session as to what NSA, what kind of indicia NSA actually uses right now. But it's exactly that -- it's -- in telecommunications, it's not always with certainty these days exactly where a communicant is.

SEN. NELSON: But --

MR. WAINSTEIN: And we have to use the information we have to make a reasonable determination as to where that person is.

MR. McCONNELL: But if we know, we -- if the collector knows you're in the United States, it requires FISA.

SEN. NELSON: Okay. Now, if you know that two people are in the United States, and you are collecting that information in the United States, normally that would require a FISA order.

MR. McCONNELL: Yes, sir.

SEN. NELSON: Does that include if you know one of those people on the communication in the United States is a member of al Qaeda?

MR. McCONNELL: Yes, sir.

SEN. NELSON: It still does. Okay.

Mr. Chairman, I want to turn back to the question that I asked before. And you stop me, as you did before, if you don't want me to proceed. But it was openly discussed in all of the public media that the 72-hour rule under current law was not obeyed with regard to the intercepts that have occurred. And my question was -- well, I first asked why, but then I asked did it in the administration. I would like an administration witness to answer if what we read in the New York Times and the Washington Post and the

L.A. Times and the Miami Herald about the 72-hour requirement not being complied with, is that true that it wasn't complied with, the law, the current law?

MR. POWELL: Senator, when you're referring to the 72-hour rule, I think you're referring to the emergency authorization provisions by which the attorney general, if all of the statutory requirements are met to the attorney general's satisfaction, he may authorize surveillance to begin and then has 72 hours after that to go to the FISA Court. If that is what you're referring to, Senator --

SEN. NELSON: Well, that's what I stated in my previous question --

MR. POWELL: Yes, Senator.

SEN. NELSON: -- when the chairman stopped me.

MR. POWELL: Senator, what the president discussed in his radio address, I believe, of December 17th, talking about one-end communications involving al Qaeda or an affiliate, those were done under the president's authorization and the president's authority were not done pursuant to FISA or attorney general emergency authorizations by which after 72 hours you would go to the FISA Court, to that extent the emergency authorizations provision of FISA was not a part of that terrorist surveillance program.

SEN. NELSON: Well, here's the trick, and I'll conclude. The trick is we want to go after the bad guys, we want to get the information that we need, but we're a nation of laws and we want to prevent the buildup of a dictator who takes the law into his own hands, saying, "I don't like that."

So now we have to find the balance. And that's what we need to craft, because there is legitimate disagreement of opinion on the interpretation that the president broke the law the last time. Senator Bond would say, no, he didn't, because he had an Article 2 constitutional right to do that.

Well, this is what the American people are scared about, that their civil rights and civil liberties are going to be invaded upon because somebody determines, outside of what the law says in black and white, that they think better than what it says. And so we've got to craft a new law that will clearly make that understandable.

Thank you, Mr. Chairman.

SEN. ROCKEFELLER: Thank you, Senator Nelson. Senator Wyden, I'll get you in just a second.

The chairman would say very strongly here at this point that this in fact a creative process, and that those who watch or listen or whatever -- it's okay that we do this. What it does say is that what we were discussing is incredibly important for the national security, as is what we're talking about, incredibly important for individual liberties. It is wholly understandable, and it is wholly predictable in this senator's view, that there would be areas where we would come to kind of a DMZ zone, unhostile, and where one side or another would get nervous.

It is the judgment of this chairman that in a situation like that, when you're dealing with people who run the intelligence, that you respect their worry, because you do not have to worry about the fact that the information will come out. Because we do have a closed hearing, and all members will be at that closed hearing. And they will hear the answers to the questions that have been asked.

So that -- I don't have a hesitation if I feel, and the vice chairman on his part has that same right. If there's a feeling that we're getting too close to the line, let's not worry too much about that. We have not crossed that line. The senator from Florida extended my cutoff, as he said, a little bit further. There was not particular objection on your part, and so the situation has been resolved.

But I just wanted to make that clear. If -- when we're in open session, this is the only committee on this side of the Capitol Building which runs into conflicts of this sort, potential conflicts of this sort. And we darn well better be very, very careful in the way that we resolve them and err in my -- and from my point of view, on the sense of caution.

Because if we're going to craft something, and Senator Bond and I have been talking about this a little bit during the hearing. If we're going to craft something which can get bipartisan support, which is what we need, we need to have not only trust but also the integrity of discourse.

Words can do great damage. They can do great good. Silence can do great damage. Silence can do great good.

So I consider all of this useful, and I now turn to Senator Wyden.

SEN. RON WYDEN (D-OR): Thank you, Mr. Chairman. I happen to agree that both you and Senator Bond have made valid points on this. And what concerns me is, too much of this is still simply too murky.

And I think, with your leave, Admiral McConnell, let me just kind of wide through a couple of the other sections that still concern me.

Section 409 on physical searches creates a new reason to hold Americans' personal information obtained in a physical search, even when a warrant is denied. And I want to kind of walk you through kind of existing law and then the change and get your reaction.

Current law allows the attorney general to authorize a secret emergency search of an American's home, provided that the government gets a warrant within three days of the search. If the arrant is denied, then information gathered in the search may not be used unless it indicates a threat of death or harm to any person. I think virtually nobody would consider that out of bounds. That's a sensible standard in current law.

But the bill would permit the government to retain information gathered in the secret search of an American's home, even if the warrant is later denied, if the government believes there is something called significant foreign intelligence information. How is that definition arrived at? What is the process for that additional rationale for keeping information on hand after a warrant is denied?

MR. McCONNELL: Sir, I'll turn to the lawyers for a more official definition of that. But the way I would interpret it as an operator is, it would be threat information, something of a planning nature that had intelligence value, that would allow us to prevent some horrendous act. So it would be something in the context of threat.

SEN. WYDEN: What amounts of an imminent act.

MR. McCONNELL: Imminent or a plan for, you know blowing -- a bridge or something of that nature.

SEN. WYDEN: I was searching for the word "imminent," and I appreciate it.

The lawyers -- I'll move on, unless you all want to add to it. But I was searching for the word "imminent." Do y'all want to that? Because I want to ask one other question.

MR. POWELL: Well, I just want to make it clear, Senator, that you did represent the proposal correctly, that the words "significant foreign intelligence information" would go broader, to just something that is imminent or a terrorist event. So the proposal is broader there, to allow the government -- retain and act upon valuable foreign intelligence information that's collected unintentionally, rather than being required to destroy it if it doesn't fall in the current exception. But you represented the proposal correctly, Senator.

SEN. WYDEN: All right. Let me ask a question now about 408, and this goes back to the point that I asked you, Admiral, earlier about -- that a section of the bill grants immunity from liability to any person who provided support to the warrantless wiretapping program or similar activities. I asked whether the immunity would apply even to persons who knowingly broke the law, and I asked what is in Section 408 that distinguishes intentional lawbreakers from unintentional ones. And I still can't find it after we've gone back and reviewed it. Can you and the lawyers point to something there -- it's at page 35, Section 408 -- that allows me to figure out how we make that distinction?

MR. POWELL: Right, Senator. 408, the liability defense -- what it would do is say that the attorney general or a designee of the attorney general would have to certify that the activity would have been intended to protect the United States from a terrorist attack.

The attorney general would actually have to enter a certification for anybody to be entitled to this defense. I don't believe the attorney general or the designee would issue such a certification for somebody who was acting in the manner that you've described.

SEN. WYDEN: So that essentially is how you would define the last seven or eight lines of page 35 is that the attorney general would have to make that certification.

MR. POWELL: That's correct, Senator. It's not a defense that somebody could just put forth without having the attorney general involved in a certification process.

SEN. WYDEN: Gentlemen, I think you've gotten the sense from the committee that one of the reasons that the bar is high now is that the American people have been told repeatedly -- both with respect to the national security letters and, I touched on earlier, the Patriot Act and other instances -- we've been told in language similar to that used today that steps were being taken to assure that we're striking the right balance between fighting terrorism and protecting people's privacy. And that is why we're asking these questions. That's why we're going to spend time wading through text.

Admiral, you've heard me say both publicly and privately, you've been reaching out to many of us on the committee to go through these specific sections. You've got a lot of reaching out to do based on what I've heard this afternoon and, I think, what I've heard colleagues say today.

But we're interested in working with you on a bipartisan basis, and I look forward to it.

Thank you, Mr. Chairman.

MR. McCONNELL: Thank you, Senator.

SEN. ROCKEFELLER: Thank you, Senator Wyden.

I'll conclude with three questions, unless the vice chairman has further questions. (Short pause.)

This would -- this is listed as all witnesses. I'd like to minimize -- a little minimization there. A criticism of the administration's bill is that while the reasons given for the bill are focused on the need to respond to the threat of international terrorism, the administration's bill would authorize warrantless surveillance of all international calls for any foreign intelligence purpose.

How would you respond to a suggestion that a more narrow approach be considered that would specifically address communications associated with terrorism, as opposed to the blanket foreign intelligence purposes in the administration's proposal?

MR. McCONNELL: Sir, if it's inside the United States, regardless, it would require a warrant, as it does today. So if it were -- if the foreign intelligence originated in a foreign location and it has to do with intelligence of interest to the United States, such as weapons of mass destruction shipment or something to do with a nation state not necessarily associated with terrorism, that would still be a legitimate foreign intelligence collection target. So something inside the United States requires a warrant. External United States, what we're arguing is it should not require a warrant, as we have done surveillance for 50 years.

SEN. ROCKEFELLER: Thank you.

Mr. Wainstein, the administration's bill would expand the power of the attorney general to order the assistance of private parties without first obtaining a judicial FISA warrant that is based on the probable cause requirements in the present law. A limited form of judicial review would be available under the administration's bill after those orders are issued.

Why is this change necessary? Has the FISA Court's review of requested warrants been a problem in the past?

MR. WAINSTEIN: Mr. Chairman, I believe what you're referring to is Section 102, large A. And what that does is it says that for those communication interceptions that no longer fall under FISA with a redefinition of electronic surveillance, that there's a mechanism in place for the attorney general to get a directive that directs a communications company to assist in that surveillance, because there's no longer a FISA Court order that can be used to -- that can be served on that company. So this way the attorney general has a mechanism to get a directive to ask a company to provide the assistance that's necessary.

If that company disagrees with that and wants to challenge that order, this proposal also sets up a mechanism by which that company can challenge that order to the FISA Court. So there is judicial review of any compulsion of a communications provider to provide communications assistance to the government.

SEN. ROCKEFELLER: And there are precedents in American law for such?

MR. WAINSTEIN: Yes, in a variety of different ways, both in the criminal side and in the national security side, yes, sir.

SEN. ROCKEFELLER: Okay. My final question is also to you, sir. The administration argues that if these FISA amendments were enacted, there could be greater attention paid to the privacy protections of persons in the United States. Among these amendments, however, are previous -- are provisions that would presumably limit the amount of information being provided to the Foreign Intelligence Surveillance Court.

The proposed amendments, for example -- and here we get back to what has already been discussed -- provide for the use of, quote, "summary description," unquote, rather than "detailed description," quote, unquote in FISA application when it comes to, quote, "the type of communications or activities to be subjected to surveillance."

Is the Department of Justice seeking to limit the information a judge of the FISA Court has available upon which to base a decision and issue and order for electronic surveillance? And if that be the case, why?

MR. WAINSTEIN: Mr. Chairman, I appreciate the question. And those specific proposed revisions essentially say that instead of providing very detailed explication of those points that you just cited, the government can provide summary information. And that's a recognition of the fact that right now the typical FISA Court package that goes to the court is, you know, 50-60 pages, something in that range. It's a huge document. And a lot of that information is completely -- or more or less irrelevant to the ultimate determination of probable cause. It needs to be there in summary fashion, but not in detailed fashion.

So that's all those streamlining provisions are doing. They're not in any way denying the FISA court the critical information they need to make the findings that are required under the statute.

And in terms of our statements that this overall bill will protect the privacy rights of Americans, frankly, it's a very practical point, which is that right now we spend a lot of time -- in the Department of Justice, NSA and the FISA Court -- focusing on FISA packages that really don't relate to the core privacy interests of Americans. They relate to these FISA intercepts, which really weren't intended to be covered by FISA. If those are taken out of FISA so that we're focusing back on privacy interests of Americans, then all that personnel, all that attention will be focused where it should be, on Americans and all Fourth Amendment interests here in the United States.

MR. POWELL: And, Senator, if I could add -- because there's a lot of attention to Department of Justice and attorney resources -- a critical piece on this is that these applications in some -- in many cases resembled finished intelligence products. The burden is on the analysts and the operators, so it's not a matter of more resources for the Department of Justice that we could bring lawyers on board and bring them in, and they would somehow magically understand the cases and be able to produce what are essentially finished intelligence products, in some cases, for the court; we think that goes where we've gotten to, and the place with the statute has gone beyond what anybody ever intended.

The burden of that falls on the analysts and operators at the -- of the intelligence community, not the lawyers, Senator. We ask the questions and we write them down and we put the packages together, but it's a huge burden to put this type of product together with people who are very limited, whose time is very limited, and they need to spend time sitting with me and Ken's staff to produce these products. So it's not just a question of Department of Justice resources -- I think that would be a solvable problem -- the issue really becomes kind of the limited analysts and operators that are working these cases in real time.

SEN. ROCKEFELLER: If the -- what you suggest is -- and I'm actually growing a little weary of this term, the "burden" -- the "burden" -- there are a lot of burdens in government, there's a lot of paperwork in government. Go work for CMS someday and you'll get a real lesson in burden. Is that what -- is the burden that you're referring to -- too much paperwork, don't have time, can't respond in time -- is that what the courts are saying or is that what you are saying?

MR. POWELL: Yeah, I think the issue is not the -- it's the issue of -- it's not the burden to focus on what the balance was struck in 1978, to focus on U.S. persons in the United States. What we have done is taken a framework that was designed to prevent domestic abuses that threatened our democratic institution. That was meant to protect against that and the abuses that happened -- and we can talk about those -- and we've just simply, because of the way technology has developed, transferred that framework to people who were never intended to be a part of that, and where that danger, frankly, is not -- does not exist.

So it's taken a framework designed to prevent domestic abuses, and because -- simply because of technological changes, transferred this to foreign entities, and I don't think anybody -- any -- I have not heard any reasonable argument that those activities directed at foreign entities not in the United States somehow present the same threats that we were concerned about domestically. So we've shifted the entire framework -- simply because of technology, we've shifted a good portion of that framework to a situation that is completely different, and we are put back in place that original balance that we believe was struck in 1978, Senator.

SEN. ROCKEFELLER: Well, it occurs to me -- and these are my closing remarks -- is that changing technology is a part of every aspect of all of our lives.

And so we all live with it every day in many ways -- some catch up, some don't. You have to be ahead of the curve, and you have to be able to respond very rapidly.

I think it's going to be very important -- and Senator Bond and I have discussed this during this hearing and before -- that we come out with a solution that works on this. I think it would be very damaging if we did not. I think it would be very damaging if we came out with a solution which went along purely partisan lines and was based upon arguments from one end to another.

Having said that, I'm not sure it's going to be easy, and what I want to -- and that's why the intelligence, the orders, the -- that we have not received chafe at the vice chairman and myself. When you're not completed -- when you're not given complete information on something which is so fundamental and where the line between privacy and security has to be so exact, then there can be a real sense of frustration if only because you fear you're not acting on complete information. It has nothing to do with our trusting of all of you. It has to do with the process which is meant to inform the intelligence committees in the Senate and the House of what the legal underpinning is.

So I would repeat my request, particularly to the director of National Intelligence, that this is a matter not just of letters that have been written and requests which have been made, but a matter of really important fundamental ability of us to work together as a committee to produce a good product. I want a product that works for America. Senator Bond wants a product that works for America. There are going to have to be some adjustments made, as there inevitably will, or else we just go on in some kind of a food fight which is no good for anybody at all.

So I would ask that cooperation, and I would renew my request for the information that I asked for in my opening statement.

SEN. BOND: Mr. Chairman, I join with you in asking for the legal justifications. Now I recognize in some attorney-client relationships the opinions reflect the negative side rather than the positive side, and I don't know what would be in those -- in that information.

But suffice it to say that we need specifically, succinctly the legal justifications and a copy of the kind of orders that went out, so we can see what went on.

On the other hand, when we're on another issue, when we're talking about FISA applications, Mr. Powell, how many FISA applications are made a year?

MR. POWELL: I think Mr. Wainstein will have the numbers. I have them in my bag, Senator. They're in a report that is publicly filed each year. I -- Ken may now have the --

MR. WAINSTEIN: I think the most recent number was 2,183 for 2006.

SEN. BOND: 2,183, and they average about 50 pages?

MR. WAINSTEIN: About that, yes, sir.

SEN. BOND: So 50 pages times that. My math is a little slow. But each year that would be over -- roughly 110,000 pages. And to go back -- each year we go back would be another 100,000. I think we ought to -- there was a question about having all FISA orders.

I think we need to come to a reasonable agreement on maybe -- I don't know where we would put 100,000 pages of orders. And I think that we need to look at that and find a way to issue a request that can be responded to and that we can handle. But I do believe very strongly that clear, succinct legal justification will -- should be shared with us when we're in the closed hearings.

And we got into the fringe areas of a lot of things that the chairman and I know why it could not be answered. And while it may appear that there was a lack of forthcoming by our witnesses, we knew -- know full well what it is that prevents your answering it. And we will look forward to getting all those answers.

And I think it will become clear to all of us, the chairman and the vice chairman and the members, when we -- when you can lay out the specific reasons that we danced around today as to why and what and where FISA needs to be changed. And I thank you, Mr. Chairman, and I thank our witnesses.

SEN. ROCKEFELLER: And the hearing is adjourned. (Sounds gavel.)

(END OF OPEN SESSION)

Permission to post received by the Federal News Service.

Modernizing the Foreign Intelligence Surveillance Act

Statement for the Record

Senate Select Committee on Intelligence

May 1, 2007

J. Michael McConnell
Director of National Intelligence

Information as of
May 1, 2007

SENATE SELECT COMMITTEE ON INTELLIGENCE
FISA MODERNIZATION

UNCLASSIFIED
STATEMENT FOR THE RECORD

INTRODUCTION

Good morning Chairman Rockefeller, Vice Chairman Bond, and Members of the Committee.

I am pleased to be here today in my role as the head of the Intelligence Community (IC) to express my strong support for the legislation that will modernize the Foreign Intelligence Surveillance Act of 1978 (FISA).

Since 1978, FISA has served as the foundation to conduct electronic surveillance of foreign powers and agents of foreign powers in the United States. My goal in appearing today is to share with you the critically important role that FISA plays in protecting the nation's security, and how I believe the proposed legislation will improve that role, while continuing to protect the privacy rights of Americans.

The proposed legislation to amend FISA has several key characteristics:

- It makes the statute technology-neutral. It seeks to bring FISA up to date with the changes in communications technology that have taken place since 1978;
- It seeks to restore FISA to its original focus on protecting the privacy interests of persons in the United States;
- It enhances the Government's authority to secure assistance by private entities, which is vital to the IC's intelligence efforts;

- And, it makes changes that will streamline the FISA process so that the IC can use FISA as a tool to gather foreign intelligence information more quickly and efficiently.

As the Committee is aware, I have spent the majority of my professional life in the IC. In that capacity, I have been both a collector and a consumer, of intelligence information. I had the honor of serving as Director of the National Security Agency (NSA) from 1992 to 1996. In that position, I was fully aware of how FISA serves a critical function in enabling the collection of foreign intelligence information.

In my first eight weeks on the job as the new Director of National Intelligence, I immediately can see the results of FISA-authorized collection activity. I cannot overstate how instrumental FISA has been in helping the IC protect the nation from terrorist attacks since September 11, 2001.

Some of the specifics that support my testimony cannot be discussed in open session. This is because certain information about our capabilities could cause us to lose capability. I look forward to elaborating further on all aspects of the issues in a closed, classified setting.

I can, however, make a summary level comment about the current FISA legislation. Since the law was drafted in a period preceding today's global information technology transformation and does not address today's global systems in today's terms, the community is significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States. We must make the requested changes to protect our citizens and the nation.

TODAY'S NATIONAL SECURITY THREATS

Because I believe that the proposed legislation will advance our ability to protect the national security, I would like to take a few minutes to discuss some of the current threats. The most obvious is the continued threat from international terrorists. Despite the fact that we are in the sixth year following the attacks of September 11, 2001, and despite the steady progress we have made in dismantling the al Qaeda organization, significant threats from al Qaeda, other terrorist organizations aligned with it, and its sympathizers remain.

Today, America confronts a greater diversity of threats and challenges to attack inside our borders than ever before. As a result, the nation requires more from our IC than ever before.

I served as the Director of NSA at a time when the IC was first adapting to the new threats brought about by the end of the Cold War. Moreover, these new threats are enhanced by dramatic, global advances in telecommunications, transportation, technology, and new centers of economic growth.

Although the aspects of Globalization are not themselves a threat, they facilitate terrorism, heighten the danger and spread of the proliferation of Weapons of Mass Destruction (WMD), and contribute to regional instability and reconfigurations of power and influence — especially through increasing competition for energy.

Globalization also exposes the United States to complex counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded. Several non-state actors, including international terrorist groups, conduct intelligence activities as effectively as capable state intelligence services. Al Qaeda, and those aligned with and inspired by al Qaeda, continue to actively plot terrorist attacks against the United States, our interests and allies.

A significant number of states also conduct economic espionage. China and Russia's foreign intelligence services are among the most aggressive in collecting against sensitive and protected U.S. systems, facilities, and development projects approaching Cold War levels.

FISA NEEDS TO BE TECHNOLOGY-NEUTRAL

In today's threat environment, the FISA legislation is not agile enough to handle the country's intelligence needs. Enacted nearly thirty years ago, it has not kept pace with 21st Century developments in communications technology. As a result, FISA frequently requires judicial authorization to collect the communications of non-U.S., i.e., foreign persons, located outside the United States. Currently, FISA forces a detailed examination of four questions:

Who is the target of the communications?
Where is the target located?
How do we intercept the communications?
Where do we intercept the communications?

This analysis clogs the FISA process with matters that have little to do with protecting privacy rights of persons inside the United States. Modernizing the FISA would greatly improve the FISA process and relieve the massive amounts of analytic resources currently being used to craft FISA applications.

FISA was enacted before cell phones, before e-mail, and before the Internet was a tool used by hundreds of millions of people worldwide every day. When the law was passed in 1978, almost all local calls were on a wire and almost all long-haul communications were in the air, known as "wireless" communications. Therefore, FISA was written to distinguish between collection on a wire and collection out of the air.

Now, in an age of modern telecommunications, the situation is completely reversed; most long-haul communications are on a wire and local calls are in the air. Think of using your cell phone for mobile communications.

Communications technology has evolved in ways that have had unforeseen consequences under FISA. Technological changes have brought within FISA's scope communications that the IC believes the 1978 Congress did not intend to be covered. In short, communications currently fall under FISA that were originally excluded from the Act.

The solution is to make the FISA technology-neutral. Just as the Congress in 1978 could not anticipate today's technology, we cannot know what changes technology may bring in the next thirty years. Our job is to make the country as safe as possible by providing the highest quality intelligence available. There is no reason to tie the nation's security to a snapshot of outdated technology.

Communications that, in 1978, would have been transmitted via radio or satellite, are transmitted principally via fiber optic cables. While Congress in 1978 specifically excluded from FISA's scope radio and satellite communications, certain fiber optic cable transmissions currently fall under FISA's definition of electronic surveillance. Congress' intent on this issue is clearly stated in the legislative history:

"the legislation does not deal with international signals intelligence activities as currently engaged in by the National Security Agency and electronic surveillance conducted outside the United States."

Similarly, FISA places a premium on the location of the collection. Legislators in 1978 could not have been expected to predict an integrated global communications grid that makes geography an increasingly irrelevant factor. Today a single communication can transit the world even if the two people communicating are only a few miles apart.

And yet, simply because our law has not kept pace with our technology, communications intended to be excluded from FISA, are included. This has real consequences to our men and women in the IC working to protect the nation from foreign threats.

FOREIGN INTELLIGENCE COLLECTION UNDER FISA

Today, IC agencies may apply, with the approval of the Attorney General and the certification of other high level officials, for court orders to collect foreign intelligence information under FISA. Under the existing FISA statute, the IC is often required to make a showing of probable cause, a notion derived from the Fourth Amendment, in order to target for surveillance the communications of a foreign person overseas.

Frequently, although not always, that person's communications are with another foreign person overseas. In such cases, the current statutory requirement to obtain a court order, based on a showing of probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security.

This is a point worth emphasizing, because I think many Americans would be surprised at what the current law requires. To state the case plainly: there are circumstances under which when the Government seeks to monitor, for purposes of protecting the nation from terrorist attack, the communications of **foreign** persons, who are physically located in **foreign** countries, the Government is required under FISA to obtain a court order to authorize this collection. We find ourselves in this position because the language in the FISA statute, crafted in 1978, simply has not kept pace with the revolution in communications technology.

Moreover, this Committee and the American people should be confident that the information the IC is seeking is **foreign intelligence** information. Writ large, this includes information relating to the capabilities, intentions and activities of foreign powers, organizations or person, including information on international terrorist activities. FISA was intended to permit the surveillance of foreign intelligence targets, while providing appropriate protection through court supervision to U.S. citizens and to other persons in the United States.

While debates concerning the extent of the President's constitutional powers were heated in the mid-1970s, as indeed they are today, we believe that the judgment of Congress at that time was that FISA’s regime of court supervision was focused on situations where Fourth Amendment interests of persons in the United States were implicated. It is important to note that nothing in the proposed legislation changes this basic premise in the law.

Another thing that this proposed legislation does **not** do is change the law or procedures governing how NSA, or any other government agency, treats information concerning United States persons. For example, during the course of its normal business under current law, NSA will sometimes encounter information to, from or about U.S. persons. Yet this fact does not, in itself, cause the FISA to apply to NSA's overseas surveillance activities.

Instead, at all times, NSA applies procedures approved by the U.S. Attorney General to all aspects of its activities that minimize the acquisition, retention and dissemination of information concerning U.S. persons. These procedures have worked well for decades to ensure the constitutional reasonableness of NSA's surveillance activities, and eliminate from intelligence reports incidentally acquired information concerning U.S. persons that does not constitute foreign intelligence.

Some observers may be concerned about "reverse targeting" in which the target of the electronic surveillance is really a person in the United States who is in communication with the nominal foreign intelligence target overseas. In such cases, if the real target is in the United States, FISA would require the IC —to seek approval from the FISA Court in order to undertake such electronic surveillance.

In short, the FISA's definitions of "electronic surveillance" should be amended so that it no longer matters how collection occurs (whether off a wire or from the air). If the subject of foreign intelligence surveillance is a person reasonably believed to be in the United States or if all parties to a communication are reasonably believed to be in the United States, the Government should have to go to court to obtain an order authorizing such collection. If the government seeks to acquire communications of persons outside the United States, it will continue to be conducted under the lawful authority of Executive Order 12333, as they have been for decades.

SECURING ASSISTANCE UNDER FISA

The proposed legislation reflects that it is vitally important that the Government retain a means to secure the assistance of communications providers. As Director of NSA, a private sector consultant to the IC, and now Director of National Intelligence, I understand that in order to do our job, we frequently need the sustained assistance of those outside of government to accomplish our mission.

Presently, FISA establishes a mechanism for obtaining a court order directing a communications carrier to assist the Government with the exercise of **electronic surveillance** that is subject to Court approval under FISA. However, as a result of the proposed changes to the definition of electronic surveillance, FISA does not provide a comparable mechanism with respect to authorized **communications intelligence** activities. The proposal would fill this gap by providing the Government with means to obtain the aid of a court to ensure private sector cooperation with lawful intelligence activities.

This is a critical provision that works in concert with the proposed change to the definition of "electronic surveillance." It is crucial that the government retain the ability to ensure private sector cooperation with activities that are "electronic surveillance" under current FISA, but that would no longer be if the definition were changed. It is equally critical that private entities that are alleged to have assisted the IC in preventing future attacks on the United States be insulated from liability for doing so. The draft FISA

Modernization proposal contains a provision that would accomplish this objective.

THE FISA PROCESS SHOULD BE STREAMLINED

In addition to updating the statute to accommodate new technologies, protecting the rights of people in the United States, and securing the assistance of private parties, the proposed legislation also makes needed administrative changes. These changes include:

(1) streamlining applications made to the FISA Court, and (2) extending the time period the Department of Justice has to prepare applications following Attorney General authorized emergency collection of foreign intelligence information.

The Department of Justice estimates that these process-oriented changes potentially could save thousands of attorney work hours, freeing up the Justice Department's National Security lawyers and the FISA Court to spend more of their time and energy on cases involving United States persons - - precisely the cases we want them to be spending their efforts on. And, if we combine the streamlining provisions of this bill with the technology-oriented changes proposed, the Intelligence Community will be able to focus its operational personnel where they are needed most.

FISA WILL CONTINUE TO PROTECT CIVIL LIBERTIES

When discussing whether significant changes to FISA are appropriate, it is always appropriate to thoughtfully consider FISA's history. Indeed, the catalysts for FISA's enactment were abuses of electronic surveillance that were brought to light. The revelations of the Church and Pike committees resulted in new rules for U.S. intelligence agencies, rules meant to inhibit abuses while preserving our intelligence capabilities. I want to emphasize to this Committee, and to the American people, that none of the changes being proposed are intended to, nor will have the effect of, disrupting the foundation of credibility and legitimacy that FISA established.

Instead, we will continue to conduct our foreign intelligence collection activities under robust oversight that arose out of the Church and Pike investigations and the enactment of FISA. Following the adoption of FISA, a wide-ranging, new intelligence oversight structure was built into U.S. law. A series of laws and Executive Orders established oversight procedures and substantive limitations on intelligence activities. After FISA, the House and Senate each established intelligence oversight committees. Oversight mechanisms were established within the Department of Justice and within each intelligence agency – including a system of inspectors general.

More recently, additional protections have been implemented community-wide. The Privacy and Civil Liberties Oversight Board was established by the Intelligence Reform and Terrorism Prevention Act of 2004. The Board advises the President and other senior executive branch officials to ensure that concerns with respect to privacy and civil liberties are appropriately considered in the implementation of all laws, regulations, and executive branch policies related to efforts to protect the Nation against terrorism. Unlike in the 1970s, the IC today operates within detailed, constitutionally-based, substantive, and procedural limits under the watchful eyes of Congress, numerous institutions within the Executive Branch, and, through FISA, the judiciary.

With this robust oversight structure in place, it also is important to ensure that the IC is more effective in collecting and processing information to protect Americans from terrorism are other threats to the security of the United States. FISA must be updated to meet the new challenges faced by the IC.

The Congressional Joint Inquiry Commission into IC Activities Before and After the Terrorist Attacks of September 11, 2001, recognized that there were systemic problems with FISA implementation. For example, the Commission noted that "there were gaps in NSA's coverage of foreign communications and FBI's coverage of domestic communications." As a result of these and other reviews of the FISA process, the Department of Justice and IC have continually sought ways to improve.

The proposed changes to FISA address the problems noted by the Commission. At the same time, a concerted effort was made in our proposal to balance the country's need for foreign intelligence information with the need to protect core individual civil rights.

CONCLUSION

This proposed legislation seeks to accomplish several goals:

- First, the changes proposed are intended to make FISA technology-neutral, so that as communications technology develops - - which it absolutely will - - the language of the statute does not become obsolete.

- Second, this proposal is not intended to change privacy protections for Americans. In particular, this proposal makes no changes to the findings required to determine that a U.S. person is acting as an agent of a foreign power. The proposal returns the FISA to its original intent of protecting the privacy of persons in the United States.

- Third, the proposed legislation enhances the Government's ability to obtain vital assistance of private entities.

- And fourth, the proposed legislation allows the Government to make some administrative changes to the way FISA applications are processed. As Congress has noted in its reviews of FISA process, streamlining the FISA process makes for better government.

This Committee should have confidence that we understand that amending FISA is a major proposal. We must get it right. This proposal is being made thoughtfully, and after extensive coordination for over a year.

Finally, I would like to state clearly my belief that bipartisan support for bringing FISA into the 21st Century is essential. Over the course of the last year, those working on this proposal have appeared at hearings before Congress, and have consulted with Congressional staff regarding provisions of this bill. This consultation will continue. We look to the Congress to partner in protecting the nation. I ask for your support in modernizing FISA so that it will continue to serve the nation for years to come.

As I stated before this Committee in my confirmation hearing earlier this year, the first responsibility of intelligence is to achieve understanding and to provide warning. As the new head of the nation's IC, it is not only my desire, but my duty, to encourage changes to policies and procedures, and where needed, legislation, to improve our ability to provide warning of terrorist activity and other threats to our security.

I look forward to answering the Committee's questions regarding this important proposal to bring FISA into the 21st Century.

Exhibit 5

PRESS ROOM
U.S. DEPARTMENT OF THE TREASURY

FROM THE OFFICE OF PUBLIC AFFAIRS

August 1, 2002
PO-3315

Testimony of
Kenneth W. Dam
Deputy Secretary, Department of the Treasury
before the
Senate Committee on Banking, Housing, and Urban Affairs
Subcommittee on International Trade and Finance
August 1, 2002

Chairman Bayh and distinguished members of the Senate Subcommittee on International Trade and Finance, thank you for inviting me to testify about the misuse of charities by terrorist organizations to raise and move money. This is an important and complex issue. I applaud the Subcommittee for focusing on it. And I appreciate the leadership you have provided, Mr. Chairman, on this and related issues.

The financial front of the war on terror is a particularly important issue for the Treasury Department. Secretary O'Neill is the Administration's principal spokesman for the financial front of the war. As his Deputy, I chair a high-level interagency committee that sets strategic priorities for the financial front. Our General Counsel, David Aufhauser, chairs the National Security Council's interagency policy coordination committee on terrorist finance. Our Under Secretary for Enforcement, Jimmy Gurulé, leads our enforcement bureaus including the United States Customs Service, the United States Secret Service, and FinCEN, as well as our Office of Foreign Assets Control as they fight terrorist financing. Our Under Secretary for International Affairs, John Taylor, works to build and maintain the international coalition against terrorist finances. Our Under Secretary for Domestic Finance, Peter Fisher, also works to help implement the USA PATRIOT Act, and to help protect our nation's critical financial infrastructure. And, of course, we have many, many employees who are working hard and, in some cases, putting their lives at risk to fight the financing of terror.

Our first actions after the tragedy of September 11 were to identify known terrorists and terrorist entities, freeze their assets in the US, and work with our allies to extend those freezes world wide. As you know, we have obtained significant results in this effort, blocking over $112 million dollars globally and forging a coalition of support that includes all but a handful of countries.

Since these first actions, our fight against the financing of terror has expanded to the abuse of charities. As Secretary O'Neill has said, few actions are more reprehensible than diverting money intended for charity and using it to support hatred and cruelty. Such abuse corrupts the sanctity of charitable giving, diverts funds and resources from those in need, betrays the trust and goodwill of donors, and is a danger to us all.

We are addressing this problem at several levels. We are stopping the flow of funds by freezing the assets of charities that are supporting terrorist groups as well as aggressively investigating suspected abuses of charities. We also work with countries around the world to help raise standards of oversight and accountability for charities. In this work we are guided always by two principles: (1) preventing the abuse of charities for terrorist purposes; and (2) preserving the important role that charities play throughout the world.

Before I detail these efforts and address the specific topics raised in your invitation letter, allow me to update you briefly on the efforts the Treasury Department has taken, in cooperation with our sister agencies and departments, to combat terrorist financing.

Achievements in Financial Aspects of U.S. Anti-Terrorism Initiatives

As you know, our priority is to prevent terrorist attacks by disrupting terrorist finances. As the President has said, we seek to "starve the terrorists of funding."

I just noted that, since September 11th, the United States and other countries have frozen more than $112 million in terrorist-related assets. More importantly, we have cut the flow of terrorist money through funding pipelines, as in the case of Al-Barakaat's worldwide network which was channeling as much as $15 to $20 million to al Qaida a year. Where warranted, we have also unblocked funds. For example, $350 million in Afghan government assets that had been protectively frozen in connection with the Taliban sanctions, mostly before September 11, have now been returned to the legitimate Afghanistan government.

We have received strong international cooperation in this effort. All but a handful of countries and jurisdictions have pledged support for our efforts, over 160 countries have blocking orders in force, hundreds of accounts worth more than $70 million have been blocked abroad, and foreign law enforcement have acted swiftly to shut down terrorist financing networks. The United States has often led these efforts, but there have also been important independent and shared initiatives. On March 11, 2002, the United States and Saudi Arabia jointly designated two branches of a charity, and on April 19, 2002, the G7 jointly designated nine individuals and one entity. These efforts have been bolstered by actions from the European Union which has issued three lists of designated terrorists and terrorist groups for blocking.

In addition to these efforts, we work with countries daily to get more information about their efforts and to ensure that the cooperation is as deep as it is broad. We are also providing technical assistance to a number of countries to help them develop the legal and enforcement infrastructure they need to find and freeze terrorist assets.

We have also had success pursuing international cooperation through multilateral forums including the U.N., the G7, the G20, the Financial Action Task Force (FATF), the Egmont Group, and the international financial institutions to combat terrorist financing on a global scale. In particular, Treasury continues to play a strong leadership role in FATF, a 31-member organization dedicated to the international fight against money laundering. As this Committee knows, in late October 2001, the United States hosted an Extraordinary FATF Plenary session, at which FATF established eight Special Recommendations on Terrorist Financing, including a recommendation regarding the need to regulate non-profit organizations. These recommendations quickly became the international standard on how countries can ensure that their financial regimes are not being abused by terrorist financiers.

Our law enforcement efforts also have proven fruitful. Treasury's Operation Green Quest, a multi-agency terrorist financing task force, was established in October 2001 to identify, disrupt, and dismantle terrorist financing networks by bringing together the financial expertise from Treasury and other branches of the government. Through their investigations, Operation Green Quest agents have been targeting a wide variety of systems that may be used by terrorists to raise and move funds. These systems include illegal enterprises, as well as legitimate enterprises, and charity/relief organizations (in which donations may be diverted to terrorist groups). Green Quest's work, in cooperation with the Department of Justice, has led to 38 arrests, 26 indictments, the seizure of approximately $6.8 million domestically, and seizures of over $16 million in outbound currency at the borders, including more than $7 million in bulk cash being smuggled illegally to Middle Eastern destinations. Recently, Customs, United States Secret Service, and FBI agents apprehended and subsequently indicted Jordanianborn Omar Shishani in Detroit for smuggling $12 million in forged cashier's checks into the United States. The detention and arrest of Shishani is highly significant as it resulted from the Customs Service's cross-indexing of various databases, including information obtained by the U.S. military in Afghanistan. That information was entered into Custom's "watch list," which, when cross-checked against inbound flight manifests, identified Shishani. In addition, Green Quest agents, along with the FBI and other government agencies, have traveled abroad to follow leads and examine documents.

We are confident that our efforts are having real-world effects. What I can tell you in open session is that we believe that al Qaida and other terrorist organizations are suffering financially as a result of our actions. We also believe that potential donors are being more cautious about giving money to organizations where they fear that the money might wind up in the hands of terrorists. In addition, greater regulatory scrutiny in financial systems around the world is further marginalizing those who would support terrorist groups and activities. This deterrent effect, though perhaps not quantifiable, is an essential effect of our efforts.

At the same time, I must tell you that we have much to do. Although we believe we have had a considerable impact on al Qaida's finances, we also believe that al Qaida's financial needs are greatly reduced. They no longer bear the expenses of supporting the Taliban government or of running training camps, for example. We have no reason to believe that al Qaida does not have the financing it needs to conduct at least a substantial number of additional attacks. In short, a great deal remains to be done.

The Misuse of Charities and Non-Profit Organizations

Your invitation letter requested my thoughts about the scope of the problem of terrorist abuse of charities and non-profits. Unfortunately, this is not an issue on which precise measurement is possible. We do know that the mechanism of charitable giving – *i.e.*, the collection of resources from willing donors and its redistribution to persons in need – has been used to provide a cover for the financing of terror and that it has been a significant source of funds. In certain instances the charity itself was a mere sham that existed simply to funnel money to terrorists. However, the abuse often occurred without the knowledge of donors, or even of some members of the management and staff of the charity itself. Allow me to provide some examples.

Examples of Abuse of Charities by Terrorist Groups

Example 1: Afghan Support Committee (ASC)

On January 9, 2002, the United States designated the Afghan Support Committee (ASC), a purported charity, as an al Qaida supporting entity. The ASC operated by soliciting donations from local charities in Arab countries, in addition to fundraising efforts conducted at its headquarters in Jalalabad, Afghanistan, and subsequently in Pakistan. The ASC falsely asserted that the funds collected were destined for widows and orphans. In fact, the financial chief of the ASC served as the head of organized fundraising for Osama bin Laden. Rather than providing support for widows and orphans, funds collected by the ASC were turned over to al Qaida operatives. With our blocking action on January 9, 2002, we publicly identified the scheme being used by ASC and disrupted this flow of funds to al Qaida.

Example 2: Revival of Islamic Heritage Society (RIHS)

Also on January 9, 2002, we designated the Pakistani and Afghan offices of the Revival of Islamic Heritage Society (RIHS). The RIHS is an example of an entity whose charitable intentions were subverted by terrorist financiers. The RIHS was a Kuwaiti-based charity with offices in Pakistan and Afghanistan. The Peshawar, Pakistan office director for RIHS also served as the ASC manager in Peshawar. The RIHS Peshawar office defrauded donors to fund terrorism. In order to obtain additional funds from the Kuwait RIHS headquarters, the RIHS Peshawar office padded the number of orphans it claimed to care for by providing names of orphans that did not exist or who had died. Funds sent for the purpose of caring for the non-existent or dead orphans were instead diverted to al Qaida terrorists. In this instance, we do not currently have evidence that this financing was done with the knowledge of RIHS headquarters in Kuwait.

Example 3: Al-Haramain Islamic Foundation

On March 11, 2002, the United States and Saudi Arabia jointly designated the Somali and Bosnian offices of the Saudi-based Al-Haramain organization. Al-Haramain is a Saudi Arabian-based charity with offices in many countries. Prior to designation, we compiled evidence showing clear links demonstrating that the Somali and Bosnian branch offices were supporting al Qaida. For example, we uncovered a history of ties between Al-Haramain Somalia and al-Qaida, the designated organization Al-Itihaad al-Islamiya (AIAI), and other associated entities and individuals. Over the past few years, Al-Haramain Somalia has provided a means of funneling money to AIAI by disguising funds allegedly intended to be used for orphanage projects or the construction of Islamic schools and mosques. The organization has also employed AIAI members. Al-Haramain Somalia has continued to provide financial support to AIAI even after AIAI was designated as a terrorist organization by the United States and the United Nations. In late-December 2001, Al-Haramain was facilitating the travel of AIAI members in Somalia to Saudi Arabia. The joint action by the United States and Saudi Arabia exposed these operations.

Preserving and Safeguarding Charities and Charitable Giving

As I stated earlier, our goal is to guard charities against abuse without chilling legitimate charitable works. Our strategic approach, as set forth in the recently published 2002 National Money Laundering Strategy, involves domestic and international efforts to ensure that there is proper oversight of charitable activities as well as transparency in the administration and functioning of the charities. It also involves greater coordination with the private sector to develop partnerships that include mechanisms for self-policing by the charitable and non-governmental organization sectors.

Domestic Front

Here at home, we are working to stem the flow of funds to terrorists through all channels. As mentioned above, we have issued blocking orders against charities and branches of charities providing support to terrorists. The three examples I cited previously all represent such blocking actions. In addition, we have blocked the assets of several other charities or groups that claimed to be providing charitable services. For example, on December 4, 2001, we blocked the assets of the Holy Land Foundation for Relief and Development, which describes itself as the largest Islamic charity in the United States. It operates as a U.S. fundraising arm of the Palestinian terrorist organization Hamas. We have also designated as terrorist supporters the Makhtab al-Khimamat/Al Kifah, a clearinghouse for Islamic charities financed directly by Usama bin Ladin and party to the 1993 World Trade Center attack; the Al Rashid Trust; the Wafa Humanitarian Organization; and the Rabita trust -- all Pakistan based al Qaida financier organizations; and the Ummah Tameer E-Nau, a Pakistani NGO which provided nuclear, biological and chemical weapons expertise to al Qaida.

In addition, we have blocked the assets of the Global Relief Foundation and the Benevolence International Foundation, under the provisions of the USA PATRIOT Act to assist the ongoing investigation of alleged links to terrorism.

Another aspect of our domestic strategy is to work within the U.S. regulatory system to ensure that charities are transparent to the maximum extent practical. In the United States, the transparency of the charitable sector is a concern of both federal and state officials, as well as of private organizations representing donors and charitable organizations. As this committee well knows, the Internal Revenue Service is the primary federal agency with oversight responsibility for charities. The IRS's responsibilities have expanded as the tax law has changed to keep up with the growth of the nonprofit sector, which now consists of more than 1.5 million tax-exempt organizations, including nearly 800,000 charities and 350,000 religiously-affiliated organizations that control $2 trillion in assets.

Under U.S. law, any person or group may establish an organization with charitable purposes, and the creators of the organization are free to choose any charitable endeavor they wish to pursue. If the organization applies to the IRS for recognition of tax-exempt status, and shows that it meets the requirements of Section 501(c)(3) of the Internal Revenue Code (IRC), it will be recognized exempt until it ceases to exist or until the IRS determines it no longer meets the requirements and revokes exempt status. A charity may have its Section 501(c)(3) application denied or its existing tax-exempt status revoked by the IRS if it does not comply with these standards. A "revocation" means that the organization becomes taxable and that donors will receive no tax benefits from contributions to the organization. Revocation may also cause the state in which the charity is organized to take action to ensure its assets are used for charitable purposes.

While its primary functions in this sphere are to recognize and regulate tax-exempt status and to implement those provisions of the tax code that derive from that status, the IRS also performs a crucial role in the development and dissemination of information about those charities that fall under its jurisdiction. Most IRC 501(c) (3) organizations (except for churches and certain small organizations) are required to file annual information returns showing the income, expenses, assets, and liabilities of the organization, as well as information about its programs. 501(c) (3) organizations must make their returns available to anyone who asks (except for the names of contributors) by publishing them in readily accessible electronic and hard-copy formats. The availability of information about charities' operations helps stimulate oversight by donors, the media, academia, and private organizations.

Also, State Attorneys General have statutory jurisdiction over the charitable assets of these organizations and over fundraising activities of charities. Oversight responsibilities and practices vary from state to state, but most states exercise regulatory oversight over all organizations that raise money in their state, excluding churches, synagogues, and mosques, regardless of where the charity is domiciled. State charities officials have formed a national-level organization, the National Association of State Charities Officials (NASCO - www.nasconet.org). Among other things, NASCO has promoted harmonization in registration requirements among the states, and has advanced a "Model Act Concerning the Solicitation of Funds for Charitable Purposes."

The United States also has private, non-profit organizations that work to safeguard our tradition of charitable giving. One such organization is Independent Sector, a coalition of more that 700 national organizations, foundations, and corporate philanthropy programs that collectively represent many thousands more organizations throughout the United States. Its many research activities include defining and addressing ways to improve accountability in the charitable sector. Other organizations focus on particular segments of the charitable sector. The Council on Foundations focuses on issues affecting private foundations. The Evangelical Council for Financial Accountability serves a major segment of the religious community as an accreditation organization that either grants or withholds membership based on an examination of the financial practices and accomplishments of charitable organizations that apply. It provides public disclosure of its more than 900 members' financial practices and accomplishments, including on its website, www.ecfa.org. ECFA is also the United States member of the International Committee for Fundraising Organizations (ICFO), an umbrella organization that links the accreditation organization of 10 countries (US, UK, Canada, Norway, Sweden, France, Germany, Switzerland, Austria, and the Netherlands).

Other organizations promoting transparency include the Philanthropic Research Institute, whose Guidestar organization maintains a database containing IRS filings and other financial information of over 200,000 charities. Any interested individual can access the information through its www.guidestar.org website. Another donor-information organization, the Better Business Bureau (BBB) Wise Giving Alliance, focuses on organizations that conduct broad-based fund-raising appeals. It collects and distributes information about the programs, governance, fundraising practices, and finances of hundreds of nationally soliciting charitable organizations that are the subject of donor inquiries. It asks the selected organizations for information about their programs, governance, fund raising practices, and finances, and measures the results against general guidelines and standards it has developed for measuring organizational efficiency and effectiveness. It publishes the results, including whether the selected organization refused to supply information, on its website at www.give.org.

While we are continually assessing ways to attack terrorist finances, there is no current Treasury Department proposal under consideration to modify the federal tax code for the purpose of blocking terrorist finance through charities. However, we are working with state charities officials and the private sector watchdog agencies to widen their horizons from the pursuit of fraud to the fight against terrorist finance.

International Efforts

As on all issues related to terrorist financing, our efforts to prevent the abuse of charities by terrorists can only be successful if we have international cooperation and support. As I have stated before, we cannot bomb foreign bank accounts. We need the cooperation of foreign governments to investigate and block them. The blocking actions we have taken to date were not isolated U.S. actions, as seen in the March 11, 2002, joint designation with Saudi Arabia. Each of the blocking actions we have taken to combat the abuse of charities – with the exception of the freezes in aid of US-based investigations – has been backed and echoed by our allies. I am very proud of the work that has gone into building the international coalition against financial terrorism, and would like to take this opportunity to give credit to the other agencies of the US government – including the State Department, the intelligence community, the FBI and the Department of Justice – that have helped us keep that coalition in place.

Moreover, we are working with other countries to strengthen their own internal charitable regulation regimes so that they can feel confident that their charitable communities are not being abused. We have pursued these discussions both bilaterally and multilaterally, in the Middle East, South East Asia, and Europe, as well as in the G7 and G8 processes and especially through the Financial Action Task Force (FATF). Secretary O'Neill has raised this issue directly with his counterparts on his visits to the Persian Gulf and Europe. Other countries, especially those whose cultures incorporate, encourage, and require charitable giving, are as concerned as we are that the good deeds of well-intentioned donors should not be hijacked by terrorists.

They are making progress, as even a cursory review of foreign press reports indicates. For example, on March 21, the Saudi press reported that the Saudi government had issued a regulatory decision requiring charitable societies to submit to the Saudi Foreign Ministry the details of projects they intend to finance abroad. Also in March, the Pakistani press reported on the Pakistan Center for Philanthropy, an independent, non-profit organization dedicated to improving philanthropic regulation. According to these reports, the Pakistani government asked the center to develop recommendations for a new law governing charities, NGO's, and other civil society organizations. In May, the Azerbaijani press reported that the government had submitted to parliament a new law further regulating the funding of charities and other NGO's. And in June, the Egyptian press reported that a draft law expanding government oversight of non-governmental and charitable organizations was submitted to parliament.

There is not a single correct approach to ensuring appropriate transparency and oversight of charitable organizations. Different countries attempt to do so using a variety of approaches. In some, independent charity commissions have an oversight role. In other countries, government ministries are directly involved. Moreover, in many jurisdictions, the focus of oversight has been combating fraud rather than terrorist financing. Many of the same regimes and mechanisms, however, can assist in the fight against terrorist finance as well.

We are attempting, bilaterally and multilaterally, to ensure that all jurisdictions treat the regulation of charitable institutions with the seriousness it deserves. As I mentioned earlier, one of the eight special counter-terrorism recommendations adopted at the October 2001 plenary session of FATF specifically called on member countries to ensure that charities and other NGOs should not be abused for the furtherance of terror, and the United States is taking the lead within FATF to develop specific best practices to ensure transparency, accountability, and enforcement of regulations over charities.

Additional Authority to Prevent the Misuse of Charities

Mr. Chairman, your invitation letter inquires whether the Administration needs additional authorities to prevent the abuse of charities. As you know, on December 20, 2001, Congress passed the "Victims of Terrorism Tax Relief Act of 2001" in which there were revisions of some elements of the tax code. An important change in the tax-related laws involved the expansion of the availability of tax returns and return information under Section 6103 for purposes of investigating terrorist incidents, threats, or activities, and for analyzing intelligence concerning terrorist incidents, threats, or activities. The ability to access and consolidate all relevant financial information in order to uncover terrorist networks and support cells is crucial to our overall efforts. In this context, it is important to our efforts to ensure that charities are not being abused by terrorist groups and supporters.

Though we are exploring ways to make our efforts more efficient and effective, we do not see a particularized need at this time to ask this Committee and Congress for additional authority. We look forward to working with you when we identify necessary changes to make our efforts most effective.

Conclusion

Mr. Chairman, this concludes my formal testimony. I would be pleased to answer any questions that you, or members of the Committee, may have regarding the Administration's goals and policies regarding the abuse of charities by terrorist organizations as well as other issues related to terrorist financing.

Exhibit 6

Testimony of
Gary M. Bald, Acting Assistant Director
Counterterrorism Division, FBI

"Coordination of the United States' Efforts to Combat Money Laundering and Terrorist Financing"

Before the Senate Caucus on International Narcotics Control
March 4, 2004

Good morning Mr. Chairman and members of the United States Senate Caucus on International Narcotics Control. On behalf of the Federal Bureau of Investigation (FBI), I would like to express my gratitude to you for affording us the opportunity to participate in this forum and to provide comments on the FBI's achievements, together with our partners in the war on terror, in the effort to identify, dismantle and disrupt sources of terrorist financing and money laundering. I also appreciate the opportunity to highlight our efforts with regard to interagency cooperation in the battle against terrorist financing.

The fight against terrorist financing is a major front in our war on terror. We recognize that terrorists, their networks and support structures require funding in some form to exist and operate. Whether the funding and financial support is minimal or substantial, it often leaves a financial trail that can be traced, tracked, and exploited for proactive and reactive purposes. Being able to identify and track financial transactions and links after a terrorist act has occurred or a terrorist activity has been identified is important, but the key lies in exploiting financial information to identify previously unknown terrorist cells, recognizing potential terrorist activity or planning, and predicting and preventing potential terrorist acts. To this end, the FBI has bolstered its ability to effectively combat terrorism through the formation of the Terrorist Financing Operations Section (TFOS).

TFOS was created in April, 2002 to combine the FBI's traditional expertise in conducting complex criminal financial investigations with advanced technologies and the critical legislative tools provided through the USA PATRIOT Act. TFOS has built upon these established mechanisms by developing cooperation and coordination among law enforcement and intelligence agencies, both domestic and foreign, to form the preeminent terrorist financing investigative operation. In the past several months, TFOS has demonstrated its capabilities by conducting near real-time financial tracking of a terrorist cell and providing specific and identifiable information to a foreign intelligence agency, which resulted in the prevention of six, potential deadly terrorist attacks.

The TFOS mission includes: conducting full financial analysis of terrorist suspects and their financial support structures in the US and abroad; coordinating joint participation, liaison, and outreach efforts to exploit financial resources of private, government, and foreign entities; utilizing FBI and Legal Attaché expertise and relationships to fully develop financial information from foreign law enforcement and private agencies, including the deployment of TFOS personnel abroad to locations such as Iraq; working jointly with the intelligence community to fully exploit intelligence information to further terrorist investigations; working jointly with prosecutors and with the law enforcement and regulatory communities; developing predictive models and conducting data analysis to facilitate the identification of previously unknown or "sleeper" terrorist suspects; and providing the financial component to classified counterterrorism investigations in support of the FBI's counterterrorism responsibilities.

Achievements towards the identification, dismantlement and disruption of sources of terrorist financing:

Before addressing some specific, investigative accomplishments in the fight against terrorist financing since 9/11/01, it is important to mention our progress in broad areas. For instance, international awareness and cooperation on the problem of terrorist financing has reached unparalleled levels. Outreach with, and cooperation from, the private sector has been outstanding and continues to develop--particularly the level of two-way interaction between law enforcement and the private sector. The resulting ability of FBI to access and obtain information in a timely fashion has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity. Moreover, the ability to conduct near real-time monitoring of specifically identified financial activity has been invaluable not only to investigations ongoing in the US, but to foreign law enforcement and intelligence agencies in related investigations.

As an example of our successful liaison and outreach efforts, extensive training and support of international investigations by TFOS has resulted in Agent visits, exchanges and training programs involving countries in Europe, Southeast Asia, the Middle East, Africa and South America. In support of specific high profile joint terrorist financial investigative matters, a number of countries and agencies, including the United Kingdom, Switzerland, Canada and Europol, have detailed investigators to TFOS on a temporary duty basis.

TFOS has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. These joint investigations have successfully targeted the financing of several overseas Al-Qa'ida cells. Furthermore, through the assistance of relationships established with the central banks of several strategic countries, successful disruptions of Al-Qa'ida financing have been accomplished in countries such as the UAE, Pakistan, Afghanistan, Philippines and Indonesia.

As part of this effort, TFOS has developed a specific terrorist financing and money laundering crimes curriculum for international training that includes topics such as: acquiring and handling evidence in document intensive financial investigations, major case management techniques, forensic examination tools, and methods of terrorist financing. At the request of the US Department of State, TFOS and the Internal Revenue Service have provided this curriculum to ten countries in just the past year, and are scheduled to provide it to approximately 38 countries overall, identified by the National Security Council as needing law enforcement training on conducting terrorist financing investigations.

Needless to say, access to foreign banking records is often critical to effectively following terrorist money. Through these training and outreach initiatives, TFOS has been able to obtain direct access to records provided by foreign central banks in numerous countries. In return, TFOS has also been able to assist these and other countries with the reciprocal sharing of terrorism related financial information.

TFOS has cultivated and maintains a contact database of private industry and government sources and persons who can provide financial data, including near real-time monitoring of financial transactions. Many of these contacts can be reached or accessed on a 24 hour/7 days a week basis, allowing TFOS to respond rapidly to critical incidents.

Through these contacts, with appropriate legal process, and pursuant to FBI investigative guidelines, TFOS has access to data and information from a variety of entities including: Banking Institutions, the Credit/Debit Card Sector, Money Services Businesses, the Securities/Brokerages Sector, Insurance Companies, Travel Agencies, Internet Service Providers, the Telecommunications Industry, Law Enforcement, State/Federal Regulatory Agencies, Public and Open Source Data Providers, the Intelligence Community, and International Law Enforcement and Intelligence Contacts. Access to this type of information is governed by the Right to Financial Privacy Act, Fair Credit Reporting Act, and other applicable statutes. The timeliness and accessibility of the data from these sources is contingent on a variety of factors, including whether the acquisition of the information requires legal process, the search capabilities of the data provider, and the size and depth of the data request. Nevertheless, as I've noted, the ability to access and obtain this type of information in a time sensitive and urgent manner has significantly enhanced the FBI's ability to identify, investigate and resolve immediate threat situations involving potential terrorist activity.

INTERAGENCY COOPERATION

Organizational changes have taken place within the Executive Branch with respect to the investigation of terrorism financing, including the execution of a Memorandum of Agreement (MOA) between the Department of Justice (DOJ) and the Department of Homeland Security (DHS) concerning terrorist financing investigations. The MOA addressed the importance of waging a seamless, coordinated law enforcement campaign against terrorist sources of financing. Signed by Attorney General Ashcroft and Homeland Security Secretary Ridge on May 13, 2003, it designates the FBI as the lead terrorist financing investigations and operations agency, and enables DHS to focus its law enforcement activities on protecting the integrity of US financial systems. To this end, DHS implemented "Operation Cornerstone", led by Immigration and Customs Enforcement (ICE), to identify vulnerabilities in financial systems through which criminals launder their illicit proceeds, bring them to justice and work to eliminate financial infrastructure vulnerabilities. Former US Customs Service "Operation Green Quest" criminal cases having no nexus to terrorism were converted to "Operation Cornerstone", while those cases having a nexus to terrorism were transitioned to the appropriate FBI Joint Terrorism Task Force (JTTF) where participating ICE Task Force members continue to play significant roles. Ongoing and future "Operation Cornerstone" investigations that develop links to terrorism will be referred to the FBI through TFOS. ICE and TFOS are coordinating investigative initiatives that will enable ICE to identify financial systemic vulnerabilities, and which will enable TFOS to identify ties to terrorism and terrorist financing. In addition, there is a liaison from ICE assigned to TFOS, and investigators from ICE are assigned to the JTTFs. The FBI has reciprocated by assigning an FBI Agent Unit Chief to the ICE offices in Washington, D.C.

In the various 84 JTTFs throughout the United States, ICE and FBI Agents are working side by side on numerous joint investigations. The exact number of ICE and FBI Agents varies from city to city and depends largely upon the workload at each JTTF. The JTTF does not only include ICE and FBI Agents, but representatives from State and Local law enforcement agencies, and other federal agencies such as the Internal Revenue Service, Department of Defense, Department of the Treasury, Central Intelligence Agency, Postal Inspection and the Environmental Protection Agency. Every Agency has an open-ended invitation to participate in the JTTF, and FBI Special Agents In Charge are particularly encouraged to promote interagency cooperation through the JTTFs.

Information sharing is critical to all of our efforts. The intelligence community, including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, the value will not be realized or maximized absent the ability to filter the information, analyze it, and disseminate it in an appropriate manner to those who can make the best use of the information. Toward this end, TFOS participates in joint endeavors with the Treasury Department, the Department of Justice, and the Department of Homeland Security involving potential terrorist related financial transactions. TFOS also has personnel detailed to the CIA's Counter Terrorism Center, and personnel from there work directly with TFOS on financial intelligence matters.

In addition, the National Security Council (NSC) formalized the Policy Coordinating Committee (PCC) on Terrorist Financing at the end of 2001. The NSC chairs the PCC, which generally meets at least once a month to coordinate the United States government's campaign against terrorist financing. The meeting generally focuses on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

The Departments of State, the Treasury, Homeland Security and Justice also participate in an interagency Terrorist Financing Working Group, chaired by the State Department, to coordinate government efforts to identify, prioritize, assess, and assist those countries whose financial systems are vulnerable to terrorist exploitation. Groups of experts, including DOJ money laundering prosecutors, interagency law enforcement and regulatory members, have provided extensive on-the-ground assessments of such countries' vulnerabilities in an effort to develop and provide targeted training and technical assistance to those countries identified as most vulnerable.

EXAMPLES OF INVESTIGATIONS

In addition to these developments, the FBI, working in coordination with other entities of the US government, has participated in the following successes pertaining to terrorist financing:

- The FBI conducted a detailed financial investigation/analysis of the19 hijackers and their support network, following the September 11th attacks. This investigation initially identified the Al Qa'ida funding sources of the 19 hijackers in the UAE and Germany. The financial investigation also provided the first links between Ramzi Binalshibh and the 9/11/01 terrorist attacks. A continuing investigation, in coordination with the PENTTBOMB Team, has traced the origin of the funding of September 11th back to financial accounts in Pakistan, where high-ranking and well-known Al Qa'ida operatives played a major role in moving the money forward, eventually into the hands of the hijackers located in the US. As part of the 9/11/01 financial investigation, thousands of individuals and organizations were investigated in the US and abroad to determine whether they played any part in supporting the hijackers or the operation. Although the vast majority of these individuals and organizations were cleared of culpability, this process of elimination resulted in numerous other quality terrorism investigations being initiated, as well as criminal charges against hundreds of individuals for fraud and other criminal activity.

- In 2001, an FBI Joint Terrorism Task Force in Charlotte, North Carolina, utilized racketeering statutes to obtain criminal convictions and, thus, disrupt and dismantle a Hizballah procurement and fundraising cell. Twenty-four individuals were arrested for crimes including immigration fraud, visa fraud, cigarette smuggling, interstate transportation of stolen property, fraud, bank fraud, bribery, money laundering, racketeering, and providing material support to a designated terrorist organization, with the final conviction delivered in 2003. Sentences imposed range up to more than 150 years.

- In 2002, the FBI coordinated with the Treasury Department's Office of Foreign Asset Control (OFAC) to justify the blocking of Holy Land Foundation for Relief and Development (HLF) assets and the closing of its US offices, shutting down Hamas' largest fund-raising entity in the US. The HLF had been linked to the funding of Hamas terrorist activities, and in 2000, raised $13 million.

- In October 2002, the FBI and other US government agencies assisted German authorities in identifying and taking legal action against Hamas in Germany. Through the efforts of the FBI, including TFOS, exchanges with Germany led to the closure of the Al Aqsa Foundation in Germany, a suspected Hamas fundraising organization.

- In December 2002, a federal grand jury in Dallas returned an indictment against a senior leader of Hamas, Mousa Abu Marzouk, for conspiring to violate US laws that prohibit dealing in terrorist funds. Also charged and arrested by the FBI were Ghassan Elashi, the chairman of the Holy Land Foundation for Relief and Development, a charitable organization designated as a terrorist organization by the US Treasury Department's Office of Foreign Asset Control because of its fundraising activities on behalf of Hamas. Elashi and four of his brothers, all of whom are employees of the Richardson, Texas-based InfoCom Corporation, were charged with selling computers and computer parts to Libya and Syria, both designated state sponsors of terrorism. The indictment alleged that the Elashi brothers disguised capital investment from Marzouk, a specially designated terrorist for his admitted leadership role with Hamas, for their telecommunications company, InfoCom. The indictment and subsequent arrests have disrupted a US based business, which was conducting its activities with a known Hamas leader and state sponsors of terrorism.

- In January 2003, the FBI, working in conjunction with German law enforcement, arrested Mohammed Al Hasan Al-Moayad, a Yemeni national, on charges of conspiring to provide material support to Al Qa'ida and Hamas. Al-Moayad was a significant financial contributor to Al Qa'ida and Hamas, and boasted he had provided over $20 million dollars to Usama Bin Laden. Al-Moayad participated in several fund raising events at the Al Farouq Mosque in Brooklyn, NY. Al-Moayad was arrested during an undercover operation where he believed that he was to receive a large financial contribution, which he advised an FBI source would be used to support mujahideen fighters of Al Qa'ida and Hamas. Along with Al-Moayad, several of his associates in New York were arrested for violating banking reporting requirements by structuring over $300,000 in several bank accounts in the United States.

- Offices of the Benevolence International Foundation (BIF), a US based charity, were shut down and its assets and records blocked following an OFAC and FBI investigation which determined the charity was being used to funnel money to Al Qa'ida. In February 2003, Enaam Arnaout, the head of BIF, pleaded guilty to racketeering conspiracy, admitting he fraudulently obtained charitable donations in order to provide financial assistance to persons engaged in violent activities overseas.

- A criminal case against Sami Al Arian, the alleged US leader of the Palestinian Islamic Jihad (PIJ), and the World Islamic Studies Enterprise forced the closure of several front companies suspected of funneling money to support PIJ operations against Israel. In August 2002, the investigation led to the deportation of Mazen Al-Najjar, the brother-in-law of Sami Al Arian and a known PIJ member. In February of 2003, following a 50-count indictment for RICO and Material Support of Terrorism violations, the FBI arrested Al-Arian and three other US-based members of the PIJ, including Sameeh Hammoudeh, Hatim Naji Fariz, and Ghassan Ballout. The FBI also executed seven search warrants associated with this action.

- In February of 2004, the FBI executed search warrants on the Ashland, Oregon office of Al Haramain Islamic Foundation, Inc. (AHIF). AHIF is one of Saudi Arabia's largest non-governmental organizations (NGO) with offices located throughout the world. AHIF's stated mission is to provide charitable services and Islamic education around the world. Based upon AHIF's claim to be a public benefit corporation organized exclusively for religious, humanitarian, educational and charitable purposes, the IRS granted AHIF tax-exempt status. The warrants were executed to further the investigation of criminal violations of Currency and Monetary Instrument reporting requirements by AHIF principals and subscribing to a false informational tax form. The investigation specifically focuses on a series of transactions involving traveler's checks cashed out of country and the mischaracterization of funds received by AHIF.

- TFOS is assisting coalition forces in Iraq in efforts to identify, disrupt, and dismantle the financial infrastructure of terrorist groups that are, or are planning to, attack coalition forces.

- TFOS has provided operational support to FBI Field Divisions and JTTFs across the United States to enhance their intelligence/criminal investigations of individuals and groups associated with, or providing material support to, terrorist organizations and activities. This assistance is provided in the form of conducting intelligence/criminal financial investigations, financial analytical support, major case management, financial link analysis, and the deployment of teams of experts to develop investigative plans to analyze large volumes of documents and data. TFOS has provided this type of operational support in Al Qa'ida cases in Buffalo and Portland, as well as in the Richard Reid, John Walker Lindh, Al Haramain, PIJ, and Mohamed Al-Moayad cases, among many others. This type of operational support has also been provided to Divisions investigating non-governmental organizations (NGOs), such as the Holy Land Foundation for Relief and Development, Benevolence International Foundation and the Global Relief Foundation.

- Since 9/11, the U.S. Government has blocked $36.3 million in terrorist assets located domestically, while the international community has blocked over $136 million, for a total of over $172 million. The FBI has provided assistance to both its U.S. Government partners and the international community by showing the definitive links to known terrorist organizations.

- The Treasury and State Departments have issued blocking orders on the assets of more than 340 terrorists, terrorist organizations, and terrorist supporters, many of them identified by the FBI, effectively denying them access to the US financial system.

- Federal law enforcement officials, working with the FBI in the JTTFs, have arrested over 61 individuals, indicted 47 and convicted 14 in connection with terrorist financing investigations.

- US Government agencies, to include the FBI's TFOS, deployed trainers and advisers on missions to countries around the world to assist with the drafting of legislation to combat terrorist financing, strengthen bank supervision in identifying suspicious transactions, and address other financial crimes and corruption. Since 9/11/01, over 80 countries have introduced new terrorist-related legislation and approximately 84 countries established Financial Investigation Units.

As previously noted, TFOS has conducted near real-time financial tracking of a terrorist cell and provided specific and identifiable information to a foreign intelligence agency, which resulted in the prevention of six, potential deadly terrorist attacks.
It should be noted that the above examples do not include the many classified intelligence successes that have directly contributed to the prevention or disruption of terrorist activities.

The use of information technology to better identify and isolate suspicious transactions related to terrorist financing:

The FBI has a responsibility to be not only reactive but proactive, and to think strategically about potential threats and future case development. Accordingly, TFOS, together with the Counter-Terrorism Section, Criminal Division of the Department of Justice, has begun a number of proactive initiatives to identify potential terrorists and terrorist related financing activities.

The overriding goal of these projects is to proactively identify potential terrorists and terrorist related individuals, entities, mechanisms or schemes through the digital exploitation of data. To accomplish this, TFOS seeks to 1) identify potential electronic data sources within domestic and foreign government and private industry providers; 2) create pathways and protocols to legally acquire and analyze the data; and 3) provide both reactive and proactive operational, predictive and educational support to investigators and prosecutors.
Utilizing the latest computer technology available, the Counterterrorism Division serves as a proactive, financial intelligence investigative management and support team. TFOS generates leads for other FBI components and proposes and conducts proactive financial intelligence initiatives and projects. TFOS works closely with other operational units and document exploitation initiatives to ensure financial intelligence is being fully exploited and disseminated.

TFOS has conducted an extensive review of data mining software and link analysis tools currently utilized by other governmental and private industries for consideration of use by the FBI. TFOS also participates in the FBI's SCOPE Intelligence Data Warehouse (IDW) User Management Group and has been involved in the development and planning for future enhancements to the IDW. TFOS's Proactive Exploitation Group (PEG) has created an interactive, computer playbook generator that can assist investigators in determining data sources to be queried, based upon the quantity and quality of their investigative data.

TFOS has initiated several projects to integrate data from its internal financial database, open/public source data and FBI and other government data sources onto a central query platform. Through this process, and in concert with contract vendors working for the SCOPE IDW Project, TFOS has developed a process whereby it can batch query multiple databases. This has the potential to save the FBI hundreds, if not thousands, of hours of data input and query time on each occasion it is utilized. Furthermore, it facilitates rapid acquisition and sharing of information with other agencies. Through the sophisticated tools being utilized, and the matching protocols developed, TFOS can ensure each query is properly conducted and done to a best practices query standard.

Recently, TFOS utilized the batch process it developed to exploit over three thousand identifiers. The batch process accomplished in hours what would have taken TFOS personnel and FBI Field Offices over 4,300 man-hours to conduct. Furthermore, because TFOS conducted the queries in batch form, and has global access to all of the search results, previously unidentified links, patterns and associates among the data can now be extracted. Absent the batch process, this would have been extremely difficult, if not impossible, to accomplish.

TFOS has initiated a variety of proactive data mining projects to identify potential terrorists and terrorist financing. The projects were conceived in 2002 and now, with the advent of certain software tools and data access, are either being implemented or will begin shortly.

An example of this is the Terrorist Risk Assessment Model (TRAM), which seeks to identify potential terrorist and terrorism financing activity through the use of targeted, predictive pattern recognition algorithms. The project entails the compilation of past and current known data regarding individual and group terrorist activity, methodologies, demographics, financial patterns, etc., to form a predictive pattern recognition program.

It is important to understand that these projects and similar initiatives by TFOS seek only to more fully exploit information already obtained by the FBI in the course of its investigations or through the appropriate legal process, and where there is an articulated law enforcement need. TFOS does not seek access to personal or financial information outside these constraints.

National Money Laundering Strategy

With respect to the 2003 National Money Laundering Strategy, the FBI concurs with the strategy's goals and objectives. The blocking of terrorist assets worldwide, establishing and promoting of international standards for adoption by other countries to safeguard their financial infrastructures from abuse and facilitating international information are several key objectives which must be achieved if law enforcement and regulatory agencies are to have any success in stemming the flow of illegal funds throughout the world. Within the FBI, the investigation of illicit money flows crosses all investigative program lines.

The number one priority of the FBI is prevention of terrorism. To prevent terrorist acts, all investigative and analytical tools of the U.S. Government must be strategically applied, in a cohesive manner, through the JTTFs.

Our efforts to combat terrorism have been greatly aided by the provisions of the PATRIOT Act and, pursuant to the 2003 National Money Laundering Strategy, the FBI is ensuring its vigorous and appropriate application. It has already proven extraordinarily beneficial in the war on terrorism. Most importantly, the PATRIOT Act has produced greater collection and sharing of information within the law enforcement and intelligence communities.

Title III of the Act, also known as the International Money Laundering Anti-Terrorist Financing Act of 2001, has armed us with a number of new weapons in our efforts to identify and track the financial structures supporting terrorist groups. Past terrorist financing methods have included the use of informal systems for transferring value in a manner that is difficult to detect and trace. The effectiveness of such methods should be significantly eroded by the Act, which establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file Suspicious Activity Reports or SARS, and money transmitting businesses, which include any person who engages as a business in the transmission of money, to register with the Financial Crimes Enforcement Network (FinCEN) and file SARS.

There are other provisions of the Act that have considerably aided our efforts to address

the terrorist threat including: strengthening the existing ban on providing material support to terrorists and terrorist organizations; the authority to seize terrorist assets; and the power to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of funds held in a US correspondent account.
The FBI has utilized the legislative tools provided in the USA PATRIOT Act to further its terrorist financing investigations. It is important for the Committee and the American people to know that we are using the PATRIOT Act authorities in a responsible manner. We are effectively balancing our obligation to protect Americans from terrorism with our obligation to protect their civil liberties.

Terrorism represents a global problem. The FBI is committed to its U.S. and international partnerships and to effectively sharing information to protect our nation from terrorism. To meet this goal, the FBI has formed the International Terrorism Financing Working Group (ITFWG), which includes law enforcement and intelligence agency representatives from the United Kingdom, Canada, Australia and New Zealand, and addresses the international aspect of terrorist financing investigations.

Alternate Financing Mechanisms
In its latest report assessing the use of alternate financing mechanisms by terrorists, GAO recommended that, "The Director of the FBI should systematically collect and analyze data concerning terrorists' use of alternative financing mechanisms". The FBI has already implemented some measures to address the GAO's recommendation, and plans to implement additional measures by April 30, 2004 which address concerns identified in the GAO report.

The FBI has established specifically defined intelligence requirements used to guide the Bureau's collection efforts within its Office of Intelligence. As a result, we developed specific intelligence requirements, which are tied to various known indicators of terrorist financing activity.

TFOS has developed statistical queries in the FBI's CT Annual Field Office Report (AFOR) pertaining to terrorist financing. Included in this reporting are responses to the tracking, locating, and monitoring of subjects of terrorism investigations through the identification of emerging trends pertaining to terrorist financing techniques, including alternative financing mechanisms discovered through other criminal investigations.

TFOS has established the Program Management and Coordination Unit (PMCU), which will be responsible for, among other things, tracking various funding mechanisms used by many different subjects in ongoing investigations - to include alternative financing mechanisms. The PMCU will be well positioned to identify emerging trends across the spectrum of terrorist financing.

Measures to collect and analyze data concerning terrorists' use of alternative financing mechanisms will greatly enhance our ability to recognize, respond to, and ultimately disrupt or dismantle terrorist organizations reliant upon them. Through the international partnerships that we have established, additional sources from which to obtain similar information regarding alternative financing mechanisms are of great mutual benefit. The FBI intends to maintain and encourage liaison and relationships with our law enforcement colleagues both in the United States and all over the world to ensure that new methods of terrorism financing, as well as current ones, are accurately tracked and monitored.

Again, I offer my gratitude and appreciation to you, Chairman Grassley, as well as the distinguished members of this Caucus, for dedicating your time and effort to this issue, and I would be happy to respond to any questions you may have.

[Congressional Matters Index] [OPA Home]

Exhibit 7

Statement for the Record
John S. Pistole
Assistant Director, Counterterrorism Division,
Federal Bureau of Investigation

Before the
Senate Committee on Banking, Housing, and Urban Affairs

September 25, 2003

Good Morning Chairman Shelby, Senator Sarbanes, and other distinguished members of the committee. On behalf of the FBI, I would like to thank you for this opportunity to address the FBI's role in ensuring greater integrity of our country's financial institutions with respect to terrorist financing. I will discuss the FBI's efforts in identifying, tracking and dismantling the financial structure supporting terrorist groups to include forward thinking proactive and predictive capabilities. I will speak about our evolving liaison, sharing and outreach relationships with the financial community as well as with foreign governments and their respective financial and regulatory institutions (to include Saudi Arabia). I will conclude with some recent terrorist financing successes and the challenges we as well as private industry still face in following the money and obtaining and analyzing financial records, especially in emerging threat situations.

FBI CHANGE IN FOCUS

As Director Mueller stated during his June 18, 2003 testimony before the House of Representatives Committee on Appropriations it is critical that the FBI transform it's "intelligence effort from tactical to strategic..if the FBI is to be successful in preventing terrorism and more proactive in countering foreign intelligence adversaries and disrupting and dismantling significant criminal activity."

Following the events of September 11, 2001 (9/11), the FBI changed it's focus making counterterrorism it's highest priority and redirecting resources accordingly. The emphasis was placed on intelligence with prevention as our primary goal. Counter terrorism investigations have become intelligence driven. Criminal investigation into these matters is considered a tool to achieve disruption, dismantlement and prevention.

FORMATION OF TFOS

Prior to the events of 9/11, the FBI had no mechanism to provide a comprehensive, centralized, focused and pro-active approach to terrorist financial matters. While the FBI examined financial records at the time of previous terrorist attacks, as part of the investigation into each of the attacks, the events of 9/11 identified a critical need for a more comprehensive, centralized approach to financial matters. The Terrorist Financing Operations Section (TFOS) of the FBI's Counterterrorism Division was formed, immediately after 9/11, in response to this critical need. The mission of the TFOS has since evolved into a broader strategy to identify, investigate, prosecute, disrupt and dismantle incrementally, all terrorist related financial and fund-raising activities.

Identifying, tracking and dismantling the financial structure supporting terrorist groups is critical to successfully dismantling the organizations and preventing future terrorist attacks. As is the case in most investigations, locating and "following the money" plays a critical role in identifying those involved in the criminal activity, establishing links among them, and developing evidence of their involvement in the activity.

Terrorists, their networks and support structures, require funding in some form to exist and operate. Whether the funding and financial support is minimal or substantial, it usually leaves a financial trail that can be traced, tracked, and exploited for pro-active and reactive purposes. Being able to identify and track financial transactions and links after a terrorist act has occurred or terrorist activity has been identified, represents only a small portion of the mission; the key lies in exploiting financial information in efforts to identify previously unknown terrorist cells, recognize potential terrorist activity/planning, and predict and prevent potential terrorist acts.

In forming the TFOS, the FBI built upon its traditional expertise in conducting complex criminal financial investigations and long established relationships with the financial services communities in the United States and abroad. Integrating these skills and resources with the Counterterrorism Division, allows the FBI to bring its full assets to bear in the financial war on terrorism.

The TFOS is both an operational and coordinating entity with pro-active and reactive responsibilities. As a coordinating entity, the TFOS is responsible for ensuring that a unified approach is pursued in investigating terrorist financing networks. The TFOS achieves this directive by: 1) coordinating the financial aspects of FBI Field Office and Legat terrorism investigations; 2) establishing overall initiatives, policy and guidance on terrorist financing matters; 3) participating in the National Security Council's Policy Coordinating Committee (PCC) on Terrorist Financing; 4) coordinating national liaison with the financial services sector; 5) cooperating in and coordinating criminal terrorist financing investigations with the Department of Justice; and 6) providing support and training to Field Offices to include the designated Terrorism Financing Coordinator (TFC) .

It is critical that the financial aspects of terrorism investigations be adequately addressed and that a concerted, coordinated effort is made to investigate terrorist finance issues by experienced financial investigators. Rarely will a terrorist financing investigation be confined to the territory of one field office, rather they normally span not only multiple field office jurisdictions, but the globe; i.e., these types of investigations will frequently be linked to investigations and/or issues in other jurisdictions and other countries. It is imperative that these investigative efforts be effectively coordinated, placed into perspective with other counterterrorism efforts, prioritized in accordance with national and global strategies, and addressed in concert rather than in a disjointed, inefficient manner. Prior to the establishment of the TFOS, there did not exist within the

FBI a mechanism to ensure appropriate focus on terrorist finance issues and provide the necessary expertise and overall coordination to comprehensively address these matters.

So how far have we come in the war on terrorist financing since 9/11? There currently exists a much better understanding of terrorist financing methods. More sophisticated and effective processes and mechanisms to address and target terrorist financing continue to develop and evolve. Pro-active approaches are increasingly being utilized. The awareness around the world on the part of law enforcement, government agencies, regulators and policy makers, and the private sector of terrorist financing methods, suspicious financial activity and vulnerabilities is much higher since 9/11. International cooperation has reached unparalleled levels. Outreach with, and cooperation from, the private sector has been outstanding and continues to develop, particularly the level of two-way interaction between law enforcement and the private sector. The ability to access and obtain this type of information in a timely fashion has significantly enhanced the FBI's ability to identify, investigate, and resolve immediate threat situations involving potential terrorist activity. However, we still face significant challenges in obtaining and analyzing financially related records in a timely fashion, especially in emerging threat situations, which I will discuss later in my testimony. The ability to conduct near real-time monitoring of specifically identified financial activity has been invaluable to not only investigations ongoing in the US, but to foreign law enforcement and intelligence agencies in related investigations. This illustrates another example of not only more pro-active measures but also of increased cooperation and coordination with the international community.

LIAISON AND OUTREACH

Extensive training and support of international investigations by the TFOS has led to Agent visits/exchanges and training programs involving a variety of countries from Europe, Asia, the Middle East, South America, and Africa. In support of specific high profile joint terrorist financial investigative matters, a number of countries and agencies, including the United Kingdom, Switzerland, Canada, Germany and Europol, have detailed investigators to the TFOS on a TDY basis. The TFOS has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. These joint investigations have successfully targeted the financing of several overseas Al Qaeda cells, including cells located in Indonesia, Malaysia, Singapore, Spain, and Italy. We have also disrupted Al Qaeda financing in the UAE, Pakistan, Afghanistan, and Indonesia with the assistance of relationships established with authorities in those and other countries.

The TFOS has developed a specific terrorist financing/money laundering crimes curriculum for international training which includes topics such as: acquiring and handling evidence in document intensive financial investigations, major case management techniques, forensic examination tools, and methods of terrorist financing. At the request of the U.S. Department of State, the TFOS has led an interagency team to provide this curriculum to a number of countries (and is scheduled to provide to approximately 38 countries) identified as needing law enforcement training on conducting terrorist financing investigations.

Through these training and outreach initiatives the TFOS has been able to build relationships with foreign counterparts that improves the FBI's ability to obtain access to financial records held by foreign financial institutions.

The TFOS has cultivated and maintains a contact database of private industry and government sources/persons who can provide financial data, including near real-time monitoring of financial transactions. Many of these contacts can be reached or accessed on 24 hour/7 days a week emergency basis allowing the TFOS to respond rapidly to critical incidents. In all cases, TFOS follows applicable legal procedures in obtaining access to financial data.

Through these contacts and with legal process the TFOS has access to data and information from a variety of entities including: Banking, Credit/Debit Card Sector, Money Services Businesses, Securities/Brokerages Sector, Insurance, Travel, Internet Service Providers, Telecommunications Industry, Law Enforcement, State/Federal Regulatory Agencies, Public and Open Source Data Providers, the Intelligence Community, and International Law Enforcement and Intelligence Contacts. The timeliness and accessibility of the data is contingent on a variety of factors including whether the acquisition of the information requires legal process, the search capabilities of the data provider, and the size and depth of the data request. The ability to access and obtain this type of information in a time sensitive and urgent manner has significantly enhanced the FBI's ability to identify, investigate and resolve immediate threat situations involving potential terrorist activity. For example, the ability to conduct near real-time monitoring of specifically identified financial activity has been invaluable to not only investigations ongoing in the US, but to foreign law enforcement and intelligence agencies in related investigations.

Being able to identify and track financial transactions and links after a terrorist act has occurred or terrorist activity has been identified represents only a small portion of the mission. The key lies in exploiting financial information in efforts to identify previously unknown terrorist cells, recognize potential terrorist activity/planning, and predict and prevent potential terrorist acts. Prior to 9/11, there was not enough emphasis placed on addressing the mechanisms and systems associated with terrorist financing and disrupting them before they could be utilized to further terrorist activities.

PROACTIVE TFOS PROJECTS

The TFOS has a responsibility to be not only REACTIVE but PROACTIVE as well, to think strategically about potential threats and future case development. As a result, the TFOS, together with the Counterterrorism Section (CTS), Criminal Division of the Department of Justice (DOJ), have begun a number of pro-active initiatives to identify potential terrorists and terrorist related financing activities.

The overriding goal of these projects is to identify potential terrorists and terrorist related individuals/entities, mechanisms or schemes through the digital exploitation of data. To accomplish this, the TFOS seeks to 1) identify potential data sources; 2) create pathways and protocols to legally acquire and analyze the data; and 3) provide both reactive and proactive operational, predictive and educational support to investigators and prosecutors.

It is important to understand that these projects and similar initiatives by the TFOS seek only to more fully exploit information already obtained by the FBI in the course of it's investigations or through the acquisition of new data through the appropriate channels and legal process. The FBI does not seek access to personal or financial information outside these constraints.

INFORMATION SHARING

Information sharing is critical to all of our efforts. The intelligence community, including the FBI, produces and obtains tremendous amounts of classified intelligence information. While much of the information can be of significant value in terrorist finance investigations, the value will not be realized nor maximized absent the ability to filter the information, analyze it, and disseminate it in an appropriate manner to those who can make the best use of the information. Toward this end, the TFOS participates in joint endeavors involving the CIA, FBI, Treasury Department, Department of Justice, and the Department of Homeland Security involving potential terrorist related financial transactions, in addition to other joint participation between the TFOS and the intelligence agencies. The TFOS has personnel detailed to the CIA/CTC and personnel from there work directly with the TFOS on financial intelligence matters.

A Policy Coordinating Committee (PCC) on Terrorist Financing was formalized at the end of 2001. The PCC generally meets at least once a month to coordinate the United States government's campaign against terrorist financing. The meeting generally focus on ensuring that all relevant components of the federal government are acting in a coordinated and effective manner to combat terrorist financing.

SAUDI ARABIA AND THE WAR ON TERRORISM

Following the 9/11 attacks, it became apparent that the role of Non-Governmental Organizations (NGOs) and charitable organizations, as a potential source of funding for terrorist groups, needed closer scrutiny. This included any role that may have involved Saudi Arabia or its citizens in the support of terrorism, both directly and indirectly, through the financial support of these charitable organizations.

The Kingdom of Saudi Arabia has taken important steps to deter global terrorism, and has redoubled its efforts following the deadly car bombings in the Kingdom on May 12, 2003. Prior to the May 12 bombings, Saudi Arabia put new laws and regulations in place for all charitable organizations, ensuring that they are audited to prevent the flow of funds to entities other than charity. Saudi Arabia has also strengthened its laws and regulations regarding money laundering. These efforts include new rules concerning the verification of customers' identities as well as restrictions on non-residents' ability to open accounts in the country. These measures are being reviewed this week by an international team of experts from the Financial Action Task Force.

In March 2002, Saudi Arabia and the U.S. Government jointly blocked the accounts of Bosnia and Somalia branches of Al-Haramain Islamic Foundation, and of Wa'el Hamza Julaidan, an associate of Usama bin Laden who provided financial and logistical support to Al Qaeda.

Since the May 12, 2003 bombings of the three western compounds in Riyadh, Saudi Arabia, cooperation with the Kingdom of Saudi Arabia has significantly improved. The FBI sent an investigative team to the Kingdom and worked with the law enforcement and intelligence services to conduct the appropriate post incident investigation and evidence collection. Cooperation with the Saudi Arabian government continues on this and other terrorism investigations. Saudi Arabia has contributed to the break up of a number of Al Qaeda cells, the arrests of key Al Qaeda leaders and the capture of Al Qaeda members in Saudi Arabia.

The Saudi and U.S. Governments have recently agreed to focus increased investigative attention on identifying and eliminating sources of terrorist funding within the Kingdom and around the world. The FBI and our counterparts in the Saudi Ministry of Interior have established a joint terrorism financing task force.

THE USA PATRIOT ACT AND OTHER LEGISLATION

Our efforts to combat terrorism have been greatly aided by the provisions of the PATRIOT Act. The success in preventing another catastrophic attack on the U.S. homeland would have been much more difficult, if not impossible, without the Act. It has already proved extraordinarily beneficial in the war on terrorism, and our opportunities to use it will only increase. Most importantly, the PATRIOT Act has produced greater collection and sharing of information within the law enforcement and intelligence communities.

Title III of the Act, also known as the International Money Laundering Anti-Terrorist Financing Act of 2001, has armed us with a number of new weapons in our efforts to identify and track the financial structure supporting terrorist groups. Past terrorist financing methods have included the use of informal systems for transferring value in a manner that is difficult to detect and trace. The effectiveness of such methods should be significantly eroded by the Act, which establishes stricter rules for correspondent bank accounts, requires securities brokers and dealers to file SARs, and certain money services to register with FinCEN and file SARS for a wider range of financial transactions.

There are other provisions of the Act that have considerably aided our efforts to address the terrorist threat including: strengthening the government's position in defending suits brought by those who provide material support; and the power to seize money subject to forfeiture in a foreign bank account by authorizing the seizure of a foreign bank's funds held in a U.S. correspondent account.

The FBI has utilized the legislative tools provided in the USA PATRIOT Act to further its terrorist financing investigations. Some examples of how the TFOS has used the provisions in the USA PATRIOT Act to obtain foreign bank account information by issuing subpoenas on those foreign bank's U.S. correspondent bank and to corroborate financial data obtained through criminal investigative techniques with intelligence sources. All of these techniques have significantly assisted ongoing terrorism investigations and would not have been possible, but for the enactment of the USA PATRIOT Act.

It is important for the Committee and the American people to know that the FBI is using the PATRIOT Act authorities in a responsible manner. We are making every effort to effectively balance our obligation to protect civil liberties with our obligation to protect Americans from terrorism.

TERRORIST FINANCING SUCCESSES

The FBI has achieved several recent and notable successes. These are the direct result of our ongoing efforts to cultivate more meaningful and productive international relationships, and increase emphasis on sharing relevant financial information domestically between law enforcement, government agencies, and private financial institutions. In concert with other U.S. Government agencies, the FBI has deployed advisers and trainers on numerous missions around the world to assist countries in the crafting of legislation to combat terrorist financing, further strengthen financial oversight controls, and encourage closer scrutiny of suspicious financial transactions.

On four separate occasions, the FBI has received financial information from a foreign government directly related to the funding of a pending terrorist attack. On these occasions the FBI was able to provide near real-time tracking of the funds and provide the foreign government with specific and identifiable information regarding the parties involved in the financial transactions – more explicitly the exact location and time the transactions occurred. Based on this critical information, the foreign government was able to locate members of terrorist cells and prevent them from executing their intended terrorist attacks.

In January 2003, German law enforcement authorities that had been working closely with the FBI arrested Mohammed Al Hassan Al-Moayad, a Yemeni national, on charges of conspiring to provide material support to Al Qaeda and Hamas. Al-Moayad was a significant financial contributor to Al Qaeda and Hamas and boasted that he provided over $20 million dollars to Usama bin Laden. Al-Moayad had participated in several fund-raising events at the Al-Farouq Mosque in Brooklyn, New York. Al-Moayad has been arrested and is awaiting extradition to New York from Germany.

In December 2002, a Federal grand jury in Dallas returned an indictment against a senior Hamas leader, Mousa Abu Marzouk, for conspiring to violate U.S. laws that prohibit dealing in terrorist funds. Also arrested and charged by the FBI were Ghassan Elashi, chairman of the Holy Land Foundation for Relief and Development (HLF). Elashi and four of his brothers, all of whom are employees of the Richardson, Texas, based InfoCom Corporation, were charged with selling computers and computer parts to Libya and Syria, both designated state sponsors of terrorism. The indictment alleged that the Elashi brothers disguised capital investment from Marzouk, a specially designated terrorist for his admitted leadership role with Hamas. The indictment and subsequent arrests have disrupted a U.S.-based business, which was conducting activities with a known Hamas leader, and international state sponsors of terrorism.

In support of other FBI Field Office cases, the TFOS provided intelligence and criminal financial investigative assistance through various mechanisms such as: a) financial analytical support; b) financial link analysis; c) field deployment of financial experts; and d) major case management support. This support aided investigators in a variety of cases such as:

- The FBI Joint Terrorism Task Force (JTTF) in Charlotte, N.C. utilized racketeering and terrorist financing statutes to disrupt, and then dismantle a Hizballah procurement and fund-raising network relying on interstate cigarette smuggling.
- The FBI, supported the Treasury's Office of Foreign Asset Control (OFAC), in blocking assets of U.S. offices for Holy Land Foundation for Relief and Development (HLF). This resulted in the closure of Hamas' largest fund-raising entity in the U.S. (The HLF has been linked to the funding of Hamas terrorist activities, and raised $13 million dollars of support in 2000).
- Joint FBI-OFAC cooperation shut down U.S. based offices of Benevolence International Foundation (BIF). Assets and records were blocked after it was determined that the charity was funneling money to Al Qaeda. In February 2003, Enaam Arnaout, the head of BIF, pled guilty to racketeering conspiracy and fraud charges.
- The FBI, with cooperation from the U.S. Intelligence Community and a foreign government, apprehended a principle money launderer of Usama bin Laden's, responsible for funneling approximately tens of millions of dollars through international accounts to Al Qaeda and the Taliban.
- In February 2003, the FBI arrested Sami Al Arian, the alleged leader of U.S.-based Palestinian Islamic Jihad (PIJ), and three other members of his organization. They also closed several front companies suspected of providing material support to PIJ members in operations against Israel.

PARTICIPATION OF FINANCIAL INSTITUTIONS

Since the events of 9/11, private industry and particularly the financial services industry have made great efforts to assist law enforcement in the investigation of terrorism and terrorist financing related matters. Their corporate patriotism and desire to work more closely with government in protecting America is recognized and appreciated. They are literally on the "front lines" in the financial war on terrorism. Because it takes money to travel, communicate and carry out terrorist acts it is the bank teller, manager or broker that is more likely to interact with the next terrorist or terrorist financier, maybe even before law enforcement or the intelligence community does. For this reason, it is critical that the financial services industry receive the necessary training and awareness of the "Things to Look For" as it relates to terrorism and that they have a vehicle or mechanism to report their suspicions to the government in a timely and efficient manner. This is accomplished through the use and electronic filing of SARs. Conversely, the government needs to have a way to communicate these "Things to Look For" with the private sector as well as a mechanism to publish names of individuals, entities and/or organizations reasonably suspected of engaging in terrorist activity. Outreach and training combined with the utilization of USA PATRIOT ACT Section 314(a) facilitates the timely sharing of information between law enforcement and financial institutions. As mentioned earlier, the TFOS has sponsored and participated in a series of conferences and training forums with representatives from the financial services industry and regulators to educate them of the "Things To Look For" but more coordination and law enforcement outreach is needed.

PRODUCTION OF FINANCIAL RECORDS IN ELECTRONIC FORMAT

One of the biggest challenges facing law enforcement when it comes to financial records analysis is the unavailability of financial records in electronic format. In the past, it was common for investigators to request and financial institutions to provide copies of financial records such as statements, copies of checks or deposit slips in hard-copy (i.e., paper) form. The delays inherent to their production and forwarding to law enforcement was complicated by the fact that the records were not readily accessible by the financial institution and because they are often in paper form they are not readily searchable or retrievable. This is especially true when time is of the essence during emerging threat situations where access to and analysis of the records is critical. Some financial institutions have made great strides in converting and storing their transactional and customer records in electronic format. The credit card industry is a good example of this. Many banks and institutions even allow their customers to view and download their account transactional data via the internet into financial management programs. However, others because of the nature of their business or the costs involved do not digitally store or are not capable of producing records electronically.

Future law enforcement investigations would be significantly enhanced if financial institutions were to develop and adopt standards of best practices for the storage and production of financial records in electronic format. Countless hours and resources on the part of private industry and the government could be saved if these records were stored and produced in a format that eliminated the need for investigators to re-input or type the information back into financial analysis programs.

Currently when records are not available in a digital format, we utilize high-speed scanners to scan and copy the records. Text is thereby converted to Optical Character Recognition (OCR) searchable text. By "digitizing" the documents into scanned, searchable images they become immediately available to all with a need or interest in the records. Digitizing the records not only facilitates rapid dissemination of the documents but also provides for enhanced searching and analysis. Storage, retrieval and discovery production costs are also thereby reduced. Once the records are digital, then advanced searching tools may be applied against them to identify key information, patterns or trends.

However, as long as relevant records remain in paper form whether held by the financial institution or the government, investigators are impeded in their timely dissemination and analysis. This can have an impact on our preventative efforts.

In summary, the increased promotion of anti-terrorist financing training both domestically and internationally would go a long way towards furthering cooperation and raising awareness of patterns in terrorist financing. Efforts to interdict illegal money remitters which undermine our financial institutions and provide a potential avenue for illicit funds to be transferred should be pursued. Finally, the production of financial records in electronic format would facilitate not only sharing and analysis, but increase our ability to tactically respond to emerging threats.

CONCLUSION

Terrorism is a global problem. The solution is grounded in what we have experienced since 9/11 - unprecedented international cooperation and coordination. The threat terrorism poses must always be considered imminent. In addition to considerable financial investigative expertise, addressing terrorism and the finances that support and propagate it requires the ability to both implement proactive and preventive approaches to disrupt and dismantle as well as the ability to conduct highly reactive immediate response financial investigations to address potential imminent threats. As stated herein and in conjunction with more and more of the international community and other aspects of the U.S. Government, the FBI has made considerable progress toward achieving and implementing these abilities.

Again, I offer my gratitude and appreciation to you, Chairman Shelby, Senator Sarbanes, and the distinguished members of the Committee, for dedicating your time and effort to this issue and I would be happy to respond to any questions you may have.

Exhibit 8

PRESS ROOM
U.S. DEPARTMENT OF THE TREASURY

FROM THE OFFICE OF PUBLIC AFFAIRS

June 16, 2004
JS-1729

Testimony of R. Richard Newcomb, Director
Office of Foreign Assets Control
U.S. Department of the Treasury
Before the House Financial Services Subcommittee on Oversight and Investigations

Introduction

Madame Chairman, members of the Committee, thank you for the opportunity to testify on the Office of Foreign Assets Control's efforts to combat terrorist support networks which forms an important part of the Treasury Department and our government's national security mission. It's a pleasure to be here, as we discuss Treasury's new office and its role in these areas. Please allow me to begin with an overview of our overall mission and conclude with our strategies for addressing the threat of international terrorism.

II. OFAC's Core Mission

The primary mission of the Office of Foreign Assets Control ("OFAC") of the U.S. Department of the Treasury is to administer and enforce economic sanctions against targeted foreign countries, and groups and individuals, including terrorists and terrorist organizations and narcotic traffickers, which pose a threat to the national security, foreign policy or economy of the United States. OFAC acts under general Presidential wartime and national emergency powers, as well as specific legislation, to prohibit transactions and freeze (or "block") assets subject to U.S. jurisdiction. Economic sanctions are intended to deprive the target of the use of its assets and deny the target access to the U.S. financial system and the benefits of trade, transactions and services involving U.S. markets. These same authorities have also been used to protect assets within U.S. jurisdiction of countries subject to foreign occupation and to further important U.S. nonproliferation goals.

OFAC currently administers and enforces 27 economic sanctions programs pursuant to Presidential and Congressional mandates. These programs are a crucial element in preserving and advancing the foreign policy and national security objectives of the United States, and are usually taken in conjunction with diplomatic, law enforcement and occasionally military action.

OFAC's historical mission has been the administration of sanctions against target governments that engage in policies inimical to U.S. foreign policy and security interests, including regional destabilization, severe human rights abuses, and repression of democracy. Recent programs in the Western Balkans, Zimbabwe, Sudan, and other regions reflect that focus. Since 1995, the Executive Branch has increasingly used its statutory blocking powers to target international terrorist groups and narcotics traffickers.

Many "country-based" sanctions programs are part of the U.S. government's response to the threat posed by international terrorism. The Secretary of State has designated seven countries -- Cuba, North Korea, Iran, Libya, Iraq, Sudan and Syria - as supporting international terrorism. Three of these countries are subject to comprehensive economic sanctions: Cuba, Iran, and Sudan (1997). Comprehensive sanctions have been imposed in the past against Libya, Iraq, and

North Korea. In addition, effective May 12, 2004, the President issued a new E.O. prohibiting specific types of transactions and exportations and importations to and from Syria due to its continued support for terrorism, its occupation of Lebanon, its pursuit of weapons of mass destruction and missile programs and its undermining of the United States and international efforts to stabilize and reconstruct Iraq.

OFAC also administers a growing number of "list-based" programs, targeting members of government regimes and other individuals and groups whose activities are inimical to U.S. national security and foreign policy interests. In addition to OFAC's terrorism and narcotics trafficking programs, these include sanctions against persons destabilizing the Western Balkans and against the regimes in Burma and Zimbabwe. OFAC also administers programs pertaining to non-proliferation, including the protection of assets relating to the disposition of Russian uranium, and to trade in rough diamonds.

III. Administration and Transparency

Organization

OFAC has grown over the past eighteen years from an office with ten employees administering a handful of programs to a major operation of 144 employees administering 27 programs. A large percentage of OFAC's professional staff have had prior professional experience in various areas of the law, finance, banking, law enforcement, and intelligence. To accomplish its objectives, OFAC relies on good cooperative working relationships with other Treasury components, federal agencies, particularly State and Commerce, law enforcement agencies, the intelligence community, domestic and international financial institutions, the business community and foreign governments.

OFAC is an organization which blends regulatory, national security, law enforcement, and intelligence into a single entity with many mandates but a single focus: effectively implementing economic sanctions programs against foreign adversaries when imposed by the President or the Congress. In order to carry out OFAC's mission, the organization is divided into ten divisions, with offices in Miami, Mexico City and Bogotá and soon to open this summer an office in Bahrain. OFAC's operations are also supported by attorneys in the Office of Chief Counsel (Foreign Assets Control). Two divisions are primarily devoted to the narcotics and terrorism programs, while others, primarily the Licensing, Compliance and Civil Penalties Divisions, are geared toward interaction with the public. It is these latter Divisions that primarily serve as OFAC's liaison with the public and figure prominently in promoting the transparency of OFAC's operations. Finally, OFAC's Enforcement Division provides crucial liaison with the law enforcement community.

Licensing Division

OFAC's licensing authority serves to "fine tune" or carve out exceptions to the broad prohibitions imposed under sanctions programs, ensuring that those transactions consistent with U.S. policy are permitted, either by general or specific license. For example, working closely with the Department of State, the Licensing Division played a critical role in issuing specific licenses to facilitate humanitarian relief activity by U.S. non-governmental organizations in the wake of the Bam earthquake in Iran. The primary focus of OFAC Licensing involves the country-based programs, primarily Cuba and Iran. Major areas of activity include issuing advisory opinions interpreting the regulations; processing license applications for exports of agricultural products, medicine and medical devices to Iran and Sudan pursuant to the Trade Sanctions Reform and Export Enhancement Act of 2000; license applications pertaining to travel and activities involving Cuba; applications to unblock funds transfers blocked by U.S. financial institutions; and the preparation of numerous legal Notices continuing statutory authority for OFAC's programs and semiannual reports to the Congress on their administration. Licensing activity involving the list-based programs centers primarily on the authorization of payment for legal services provided to blocked persons. OFAC's Miami Office, which coordinates Cuba travel licensing, compliance and enforcement matters, also reports primarily to the Licensing Division.

The Licensing Division reviews, analyzes and responds to more than 25,000 requests per year for specific licenses covering a broad range of trade, financial and travel-related transactions, including those related to the exportation and importation of goods and services and the provision of humanitarian and banking and financial services. It also provides written and oral guidance to the public and private sectors on the application of OFAC's regulatory programs to specific facts and circumstances. Redacted versions of interpretive rulings prepared by the Licensing Division are published on OFAC's website. During FY 2003, the Licensing Division made substantial progress in reducing the overall response time to incoming correspondence, primarily through a net increase of staff of 11 FTEs and conversion to an Oracle database and the use of that database for effective case management. The Licensing Division is also currently implementing a new integrated voice response system to more efficiently handle the large volume of calls it receives from the public.

Compliance Division

OFAC Compliance adds a unique dimension to the war against terrorists and against other sanctions targets. Working with the regulatory community and with industry groups, it expeditiously formats and makes information public through appropriate channels in appropriate formats to assure that assets are blocked and the ability to carry out transactions through U.S. parties is terminated. It is always aware that "time is of the essence" and, if a new enemy were to appear tomorrow, OFAC is confident that it would be able to implement a new sanctions program within 24 hours even in a crisis environment. Our Compliance team is "in the trenches," so to speak, and provides a unique service through its toll-free telephone "hotline" giving real-time guidance on in-process transactions. As a result of its efforts every major bank, every major broker-dealer, and more and more industry professionals use software to scan and interdict transactions involving sanctions targets. OFAC's hotline averages 1,000 calls per week with at least $1 million and sometimes as much as $35 million in appropriately interdicted items each week. Recently, for example, OFAC worked with a US bank to block a wire transfer for close to $100,000 originating from a suspect and going to an organization associated with a Specially Designated Global Terrorist organization which we had named.

OFAC uses multiple formats and multiple platforms to get information out on its targets and - its programs - including on our website which now has over 1,000 documents, over a million hits per month, and over 15,000 email subscribers--so that banks, broker-dealers, and others can stop transactions in mid-stream.

OFAC's Compliance Division also runs more than 100 training sessions per year around the country and follows up with cases based on regulatory audits and blocked and rejected items which have resulted in 4,250 administrative subpoenas, 3,500 warning letters, and hundreds and hundreds of referrals for Enforcement or Civil Penalties action over the past five years.

Its positioning within the Treasury Department provides OFAC's Compliance with an invaluable capability to dialogue with and oversee industry groups as diverse as banking and securities, exporters and importers, travel service providers, insurers, and even credit bureaus and retailers.

Civil Penalties Division

OFAC's Civil Penalties Division acts as the civil enforcement arm of OFAC by imposing civil penalties for violations of OFAC programs. Penalties range from $11,000 to $1.075 million. Since 1993, the Division has collected nearly $30 million in civil penalties for sanctions violations and has processed more than 8,000 matters.

The Division reviews evidence and determines the appropriate final OFAC penalty action -- either a settlement, a penalty imposition, or the decision not to impose a penalty. It also grants requests for an agency hearing before an administrative law judge (ALJ) in cases under the Trading With the Enemy Act (TWEA). Four ALJs have contracted with OFAC to hear such cases. In addition to ALJ hearings and the administrative civil penalty process, OFAC's Civil Penalties Division resolves civil enforcement cases in conjunction with criminal prosecutions by the Justice Department. OFAC also enters into global settlements of violations in forfeiture actions brought by the U.S. Customs and Border Protection (CBP) and works closely with CBP's Office of Regulations and Rulings and the Fines, Penalties and Forfeitures Offices nation wide.

The Civil Penalties Division publishes information on completed settlements and penalty impositions on OFAC's Penalties Disclosure Website. Providing additional transparency, as recommended by the Judicial Review Commission, OFAC has published in the Federal Register its Enforcement Guidelines with Penalty Mitigation Guidelines.

Enforcement Division

OFAC Enforcement concentrates on providing advice and assistance concerning criminal investigations and investigates civil violations of OFAC's regulations and statutes.

- Criminal investigations. OFAC Enforcement officers provide expert advice and assistance to Assistant United States Attorneys and criminal investigators from the FBI, Bureau of Immigration and Customs Enforcement (ICE) and the Department of Commerce's Office of Export Enforcement (OEE) in the investigation of suspected criminal violations of OFAC programs. The FBI has primary investigative authority for terrorism cases, while ICE conducts most investigations dealing with trade-related transactions. OFAC's long-standing and close relationship with ICE, and its predecessor office the US Customs Office of Investigation, has continued after the transfer of Customs to the Department of Homeland Security ("DHS"). This relationship works very well. ICE has field offices nationwide, covering all ports of entry, and agents assigned as attaches for overseas investigative coverage. ICE agents, along with inspectors from the CBP at DHS, have seizure authority at U.S. ports and they are the front line of OFAC's efforts to interdict unlicensed goods being exported to, or imported from, sanctioned countries or persons. Since 1995, there have been approximately 68 cases that resulted in criminal enforcement action for TWEA and the International Emergency Economic Powers Act ("IEEPA") violations.

- Civil Investigations. The Enforcement Division conducts civil investigations as a result of voluntary disclosures, informant information, internal research by OFAC staff, and referrals from ICE and other agencies. The Division currently has more than 2600 civil cases opened. These cases range from complex export, reexport and other trade transactions, to violations of OFAC Cuba travel restrictions. Most such cases result in an internal referral to the Civil Penalties Division for the possible imposition of civil penalties.

- Domestic Blocking Actions. OFAC officers serve blocking notices and work to ensure the blocking of assets of entities in the United States that are designated under the Foreign Terrorist, Narcotics and country programs. These actions are accomplished with the assistance of special agents from the FBI and ICE as needed.

- Law Enforcement Outreach Training. OFAC provides sanctions enforcement training to ICE agents and CBP inspectors on a monthly basis through in-service training courses at the Federal Law Enforcement Training Center and at field offices and ports nation-wide. We have also provided training presentations to agents and analysts at FBI Headquarters and at the FBI Academy at Quantico, VA.

Transparency and Outreach

In January 2001, the Judicial Review Commission on Foreign Asset Control submitted its final report to the Congress, making several recommendations with respect to OFAC. While some were specific to the Foreign Narcotics Kingpin Designation Act and OFAC's designation authority generally, others pertained to the '"transparency" of OFAC's operations and decision making standards in order to facilitate greater understanding of, and compliance with, the sanctions laws [OFAC] administers." In response to the Commission's report, OFAC and the three Divisions described above have taken several measures to enhance the transparency of OFAC's operations. Central to this initiative is the use of OFAC's website, administered by the Compliance Division, which currently contains more than 1,000 documents, including 96 program brochures, guidelines and general licenses, 12 industry brochures, and over 200 legal documents. Website usage statistics indicate in excess of 1.3 million hits per month. OFAC also publishes reports, speeches, and Congressional testimony on its website. Included among the reports are quarterly reports to the Congress on the administration of the licensing regime pertaining to the exportation of agricultural products, medicine and medical devices to Iran, Sudan, and, until recently, Libya. OFAC's Terrorist Assets Reports for 2001 through 2003 are also available.

Interpretive rulings in redacted format prepared by the Licensing Division are published on the website, extending the benefit of what had previously been private guidance. OFAC has also published 95 questions of general applicability frequently asked by the public about OFAC and its programs.

Publication of various OFAC guidelines is also an important component of the transparency initiative. Along with the Enforcement Guidelines, OFAC has issued comprehensive application guidelines pertaining to the authorization of travel transactions involving Cuba. These guidelines were instrumental in reducing a backlog of license applications in this category from more than four hundred cases to fewer than one hundred, with a current average processing time per application of fewer than nine days. OFAC also issues a circular setting forth the regulatory program governing travel, carrier and funds forwarding services provided in the context of the Cuba embargo.

Responding to one of the Judicial Review Commission's recommendations, OFAC, wherever possible, has issued its regulations in the Federal Register as interim final rules allowing for public comments.

Finally, there are listings on the website for more than 100 sanctions workshops in the near future. These workshops provide a significant outreach to the financial and other communities OFAC regulates, further promoting transparency of agency operations.

IV. OFAC's Designation Programs

Designations constitute the identification of foreign adversaries and the networks of companies, other entities, and individuals that are associated with them; as a result of a person's designation pursuant to an Executive orders ("EO") or statute, U.S. persons are prohibited from conducting transactions, providing services, and having other dealings with them. Generically, those who are placed on OFAC's public list are referred to as "Specially Designated Nationals" or "SDNs." Typically, SDNs are the instrumentalities and representatives that help sustain a sanctioned foreign government or adversary and commonly include the financial and commercial enterprises, front companies, leaders, agents, and middlemen of the sanctions target. In the terrorism programs, they are known as SDGTs, SDTs and FTOs; in the narcotics programs they are SDNTs for the Colombian cartels and Tier I and

Tier II SDNTKs under the Kingpin Act. In the country programs, they are SDNs.

OFAC's International Programs Division and Foreign Terrorist Programs Division are the offices which research and identify these targets for designation.

Legal Authorities

International Emergency Economic Powers Act

In January 1995, the President first used his IEEPA authority to deal explicitly with the threat to U.S. foreign policy and national security posed by terrorism, declaring a national emergency with respect to terrorists who threaten to disrupt the Middle East Peace Process. This action, implemented through Executive Order 12947, expanded the use of economic sanctions as a tool of U.S. foreign policy to target groups and individuals, as well as foreign governments. During the late 1990s, IEEPA authorities were used to issue additional Executive Orders imposing sanctions on al Qaida and Usama bin Ladin and entities or individuals that are owned or controlled by, act for or on behalf of, or that provide material or financial support to al Qaida or Usama bin Ladin.

Following this model, in October 1995, the President announced the concept of using EO 12947 as a model for targeting significant foreign narcotics traffickers centered in Colombia, i.e., the Colombian drug trafficking cartels. That IEEPA program, implemented in EO 12978 with the identification by the President of four Cali Cartel drug kingpins, has expanded into a key tool in the fight against the Colombian cartels. As of today, 14 Colombian drug kingpins, 381 entities, and 561 other individuals associated with the Cali, North Valle, and North Coast drug cartels have been designated as Specially Designated Narcotics Traffickers ("SDNTs") under EO 12978.

Authorities in Response to September 11th.

The President harnessed the IEEPA powers and authorities – as well as his authority under the United Nations Participation Act – in response to the terrorist attacks of September 11. On September 23, 2001, President Bush issued Executive Order 13224, "Blocking Property and Prohibiting Transactions with Persons Who Commit, Threaten to Commit, or Support Terrorism" declaring that the grave acts of terrorism and the threats of terrorism committed by foreign terrorists posed an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. EO 13224, as amended, authorizes the Secretaries of the Treasury and State, in consultation with the Department of Justice and the Department of Homeland Security, to implement the President's authority to combat terrorists, terrorist organizations and terrorist support networks systemically and strategically.

This order prohibits U.S. persons from transacting or dealing with individuals and entities owned or controlled by, acting for or on behalf of, assisting or supporting, or otherwise associated with, persons listed in the Executive Order. Those designated and listed under the Executive Order are known as "Specially Designated Global Terrorists" (SDGTs). Violations of the EO with respect to SDGTs are subject to civil penalties; and if the violation is willful, persons may be criminally charged. The Executive Order also blocks "all property and interests in property of [designated persons] that are in the United States or that hereafter come within the United States, or that hereafter come within the possession or control of United States persons[.]"

To date, the U.S. has designated 375 individuals and entities as SDGTs pursuant to EO 13224. More than 270 of these entities are associated with either al Qaida or the Taliban which provides the basis to propose these names to the UN 1267 Sanctions Committee for inclusion on its consolidated list of individuals and entities the assets of which UN member states are obligated to freeze in accordance with relevant United Nations Security Resolutions (UNSCRs) including resolutions1267 and, most recently, 1526. The United States has worked diligently with the UN Security Council to adopt resolutions reflecting the goals of our domestic executive orders and obligating UN member states to freeze terrorism related assets.

Rolling FTOs into SDGTs Makes War on Terrorist Infrastructure Global

On November 2, 2001, the U.S. took an additional significant step when the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, utilized the new authorities in EO 13224 to designate 22 Foreign Terrorist Organizations (FTOs) as Specially Designated Global Terrorists (SDGTs). This action expanded the War on Terrorism beyond al Qaida and the Taliban and associated individuals and entities to include Hamas, Hizballah, the FARC, the Real IRA and others. This action created a truly global war on terrorism and terrorist financing and demonstrated the USG's commitment to continue and expand its efforts against all terrorist groups posing a threat to the United States, its citizens, its interests, and its allies. Currently, there are 37 FTOs which are also designated as SDGTs.

Foreign Narcotics Kingpin Designation Act

Building on the successes of the Colombian narcotics traffickers program, in December 1999 Congress enacted the Foreign Narcotics Kingpin Designation Act (Kingpin Act), originally introduced by Senators Coverdell and Feinstein and modeled on IEEPA and OFAC's Columbia SDNT program. It provides a statutory framework for the imposition of sanctions against foreign drug kingpins and their organizations on a worldwide scale. Like its terrorism and narcotics Executive Order-based predecessors, the Kingpin Act is directed against individuals or entities and their support infrastructure, not against the countries in which they are imbedded. Since the first list of kingpins was issued, 48 foreign drug kingpins, 14 derivative companies, and 52 derivative individuals have been designated. These totals are in addition to the 14 Colombian Principal Individuals that have been designated as Colombian Specially Designated Narcotics Traffickers [SDNTs] pursuant to E.O. 12978.

Antiterrorism and Effective Death Penalty Act

In 1996, Congress passed the Antiterrorism and Effective Death Penalty Act ("AEDPA"). AEDPA makes it a criminal offense to: (1) engage in a financial transaction with the government of a country designated as supporting international terrorism; or (2) provide material support or resources to a designated Foreign Terrorist Organization (FTO).

Thirty-seven FTOs are currently subject to OFAC-administered sanctions. These FTOs have been designated by the Secretary of State in consultation with the Secretary of the Treasury and the Attorney General. Under the AEDPA and OFAC's implementing regulations, U.S. financial institutions must maintain control over all funds in which an FTO has an interest and report the existence of such funds to OFAC. OFAC works with State and Justice on FTO designations, and with the financial community, the FBI, State, and other Federal agencies in implementing the prohibitions of the AEDPA.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the USA "PATRIOT Act"), passed in October 2001, amends IEEPA to provide critical means and authority to OFAC to counter terrorist financing and their support structures. The Act has enhanced OFAC's ability to implement sanctions and to coordinate with other agencies by clarifying OFAC's authorities to block assets of suspect entities prior to a formal designation in "aid of an investigation." This critical authority helps prevent the flight of assets and prevents the target from engaging in potential damaging behavior or transactions. In addition, the PATRIOT Act explicitly authorizes submission of classified information to a court, in camera and ex parte, upon a legal challenge to a designation. This new PATRIOT Act authority has greatly enhanced our ability to make and defend designations by making it absolutely clear that

OFAC may use classified information in making designations without turning the material over to an entity or individual that challenges its designation.

OFAC'S Counter Narcotics Program

OFAC's Mission Against Foreign Drug Cartels

One of the primary missions of OFAC/IPD officers is to investigate, through both "all-source" research and extensive field work with U.S. law enforcement agents and Assistant U.S. Attorneys, and compile the administrative record that serves as the OFAC case to designate significant foreign narcotics traffickers and their networks of front companies and individuals pursuant to the Specially Designated Narcotics Traffickers (SDNT) program pursuant to EO 12978 and the Foreign Narcotics Kingpin Designation Act ("Kingpin Act").

Interagency Coordination

In its capacity to administer and enforce economic sanctions against foreign narcotics traffickers, both traditional drug cartel and narco-terrorist targets, OFAC's International Programs Division (OFAC/IPD) works extensively with other U.S. agencies in the law enforcement and intelligence communities, as well as the President's Office of National Drug Control Policy. OFAC/IPD officers regularly are requested to train DEA's financial investigators on OFAC's authorities to designate and block foreign drug cartels' financial networks under EO 12978 and the Kingpin Act. In addition, OFAC/IPD officers have also provided presentations for various ICE, FBI, U.S. Attorney's offices, the Department of Justice, and the Department of Defense on OFAC narcotics and other sanctions programs and how they can work jointly with a U.S. criminal investigation. OFAC continues to expand its relationships with U.S. law enforcement, including ICE, DEA, FBI, IRS Criminal Investigation and U.S. Attorney's Offices, and with other agencies including the Department of State, Department of Defense, and Central Intelligence Agency. While some formal interagency coordination is established by executive order or legislation (the Kingpin Act), in the day-to-day execution of these programs, interagency cooperation is the result of experienced OFAC/IPD officers working closely with other U.S. criminal investigators. These working relationships have led to several successful sanctions designation actions over the past few years.

OFAC's Enforcement Division and its International Programs Division have distinct but complementary relationships with the federal law enforcement community. OFAC/IPD is focused on investigations and research leading to designations, whether worked independently or jointly with federal law enforcement agencies and task forces, U.S. Attorneys offices, or other USG agencies. In the programs that OFAC enforces against foreign narcotics trafficking cartels and drug kingpins, OFAC/IPD has been working with the Department of Justice and DEA since 1995, with a significant contingent of OFAC/IPD personnel cleared to work at DEA headquarters. Over the years those working relationships have substantially broadened, bringing OFAC to the point where OFAC/IPD officers, both in the field and at headquarters, including OFAC's Attaché Offices in Bogotá and Mexico City, regularly work with OCDETF task forces, multiple U.S. Attorneys' offices, DEA, ICE, IRS–CI and the FBI, on cases and broader operations of mutual interest. This integrated operating method not only provides OFAC/IPD with better background information and evidence for its targets, but also makes OFAC's expertise in the business and financial structuring by the cartels available as a resource to law enforcement and intelligence agencies. This appropriate close working relationship with law enforcement provides a successful conduit for the sharing of information between law enforcement agencies and OFAC/IPD.

Since September 11, 2001, OFAC has played an integral role in the terrorism-related investigations being conducted throughout the law enforcement community. To coordinate efforts and actions, OFAC has detailed a full time liaison to the FBI's Terrorist Financing Operations Section (TFOS) and a weekly liaison to the Terrorist Screening Center (TSC) and participates on their interagency enforcement teams. Information obtained through close interagency coordination has been crucial in "making the case" to designate particular targets domestically and internationally. Information developed by OFAC has also proven useful for investigations being conducted by TFOS, TSC and other U.S. law enforcement agencies.

The Kingpin Act

Pursuant to section 804(a) of the Kingpin Act, the Secretaries of Treasury, State, and Defense, the Attorney General, and the Director of Central Intelligence must consult and provide the appropriate and necessary information to enable the President to submit a report to Congress no later than June 1 each year designating additional Kingpin Tier I targets. OFAC/IPD is responsible for coordinating the interagency process for the Kingpin Act.

On May 29, 2003, President Bush announced the names of 7 foreign persons that he determined were significant foreign narcotics traffickers, or kingpins, under the Kingpin Act. These new drug kingpins included 3 foreign groups – a Colombian narco-terrorist guerrilla army (the Revolutionary Armed Forces of Colombia or "FARC"), a Colombian narco-terrorist paramilitary force (the United Self-Defense Forces or "AUC"), and a Burmese drug trafficking ethnic guerrilla army (United Wa State Army or "UWSA"). These were the first designations of narco-terrorist groups under the Kingpin Act. The FARC and the AUC had previously been named as Foreign Terrorist Organizations by the State Department and designated as Specially Designated Global Terrorists by OFAC pursuant to EO 13224.

On June 1, 2004, President Bush announced the names of 10 foreign persons that he determined were significant foreign narcotics traffickers, or kingpins, under the Kingpin Act. These new drug kingpins included 8 individuals involved in the Mexican, Jamaican, Peruvian, Indian, and Afghanistan drug trade and 2 Mexican groups – the Arellano Felix Organization and the Carrillo Fuentes Organization. This action underscored the President's determination to do everything possible to pursue drug traffickers, undermine their operations, and end the suffering that trade in illicit drugs inflicts on Americans and other people around the world, as well as preventing drug traffickers from supporting terrorists. Concurrent with the President's Kingpin designations, OFAC blocked, in furtherance of investigation, the Peruvian airline company, Aero Continente, six other companies, and six other individuals connected to the newly named Kingpin, Fernando Zevallos.

OFAC prepares and designates "Tier II" narco-terrorist leaders under the Kingpin Act. On February 19, 2004, OFAC/IPD took action against leaders and key figures of two narco-terrorist organizations in Colombia, the FARC and the AUC. Nineteen leaders of the FARC and eighteen key figures of the AUC plus three AUC front companies were added to OFAC's list of "Tier II" individuals and entities designated under the Kingpin Act. These Kingpin Tier II designations reinforce the reality that the FARC and the AUC are not simply terrorist/guerrilla organizations fighting to achieve political agendas within Colombia. They are part and parcel of the narcotics production and export threat to the United States, as well as Europe and other countries of Latin America.

Specially Designated Narcotics Traffickers

Since the inception of the Colombia program in 1995 under Executive Order 12978, OFAC/IPD officers have identified 956 businesses and individuals as Specially Designated Narcotics Traffickers ("SDNTs") consisting of fourteen leaders of Colombia's Cali, North Valle, and North Coast drug cartels.

- North Valle Cartel links to the AUC. In October 2002, OFAC coordinated the designation of a Colombian cartel kingpin with the FBI. A joint investigation by OFAC/IPD and the FBI Miami field office led to the SDNT action against Colombia's North Valle cartel leader, Diego Leon Montoya Sanchez and a network of front companies and individuals in Colombia in conjunction with an FBI criminal asset forfeiture action in South Florida. Diego Leon Montoya Sanchez is closely associated with the AUC, a Colombian narco-terrorist organization.

- Continued Actions against the Cali Cartel. Since 2002, OFAC/IPD has worked jointly with the U.S. Attorney's Office for Middle District of Florida and Operation PANAMA EXPRESS, a multi-agency drug task force based in Tampa, Florida. A two-year investigation by OFAC/IPD officers in conjunction with the PANAMA EXPRESS task force led to the March 2003 SDNT action against two new Cali Cartel leaders, Joaquin Mario Valencia Trujillo and Guillermo Valencia Trujillo, and their financial network of 56 front companies and individuals. Joaquin Mario Valencia Trujillo is indicted in the Middle District of Florida and was recently extradited to the U.S. from Colombia.

In 2003, OFAC/IPD investigations focused on Cali cartel leaders, Miguel and Gilberto Rodriguez Orejuela. In February 2003, OFAC/IPD designated 137 companies and individuals comprising a complex financial network in Colombia and Spain controlled by Miguel and Gilberto Rodriguez Orejuela. This action exposed and isolated a parallel network of Cali cartel front companies established to evade OFAC sanctions. In March 2003, OFAC/IPD officers targeted a Colombian money exchange business and a prominent Colombian stock brokerage firm, which facilitated the Cali cartel network's financial transactions. In October 2003, OFAC/IPD designated 134 new front companies and individuals including a network of pharmaceutical companies extending from Colombia to Costa Rica, Ecuador, Panama, Peru, and Venezuela, with ties to financial companies in the Bahamas, the British Virgin Islands and Spain. These SDNT actions were the result of a three-year investigation by OFAC/IPD officers and the OFAC Attaché – Bogota.

These actions under the SDNT and Kingpin Act programs reflect the increasing cooperation, coordination and integration among the U.S. counter-narcotics agencies in the battle against international narcotics trafficking and narco-terrorism. On March 3, 2004, the U.S. Attorney for the Southern District of New York issued a joint statement with the DEA New York field office and the OFAC Director announcing the indictment of two of Colombia's most important drug kingpins, Gilberto Rodriguez Orejuela and Miguel Angel Rodriguez Orejuela, leaders of the notorious Cali Cartel, under Operation DYNASTY, a joint investigation involving the U.S. Attorney's Office for the Southern District of New York, DEA, OFAC, and Colombian authorities. Both Cali cartel leaders were designated under EO 12978 as Colombian cartel leaders in October 1995. The indictment charges the Rodriguez Orejuela brothers with money laundering conspiracy based largely upon the predicate offense of violating the IEEPA as a result of the drug kingpins' efforts to defeat OFAC's designations of many of their companies as SDNTs.

OFAC's Counter-Terrorism Program

Foundations of Terrorist Financing and Support

The threat of terrorist support networks and financing is real, and it has been OFAC's mission to help identify and disrupt those networks.

There is much we know about how radical terrorist networks were established and still thrive. OFAC's research has disclosed the overall framework of the support structures that underpin the most prominent Islamic extremist movements throughout the world. "Deep pocket" donors in the Middle East provide money either to terrorist groups directly, or indirectly through trusted intermediaries and non-governmental organizations (NGOs), including charities. These NGOs can, in turn, use the money to provide funding and logistical services directly to terrorist groups, including transportation, cover employment, and travel documentation. They also provide support indirectly by using the funds for public works projects -- wells, social centers, and clinics -- to reach disaffected populations susceptible to radicalizing influences. These projects also often include extremist religious schools, which serve as fertile recruiting grounds for new members of terrorist groups.

The terrorist networks are well-entrenched and self-sustaining, though vulnerable to

U.S., allied and international efforts. Looking forward, please allow me to explain how we have arrived at this view and present the strategy, being implemented in coordination with other components of the Treasury Department and other Federal agencies including the Departments of Defense, State, Justice, Homeland Security, the FBI, IRS Criminal Investigation, the intelligence community and other agencies, to choke off the key nodes in the transnational terrorist support infrastructure.

Research and Evidentiary Preparation

The primary mission of officers within OFAC's Foreign Terrorist Programs Division is to compile the administrative record or "evidentiary" material that serves as the factual basis underlying a decision by OFAC to designate a specific person pursuant to EO 13224 or other counter-terrorism sanctions authorities that triggers a blocking of assets and a prohibition on US persons from dealing with the designated party. OFAC officers conduct "all-source" research that exploits a variety of classified and unclassified information sources in order to determine how the activities or relationships of a specific target meet the criteria of the EO. As the implementing and administrating agency for EO 13224 and other related programs, OFAC coordinates and works with other US agencies to identify, investigate and develop potential targets for designation or other appropriate USG actions. Officers use their considerable expertise to evaluate available information in the critical process of constructing a legally sufficient evidentiary record.

More broadly, OFAC officers compile research on multiple targets to build a comprehensive schematic of the structure of particular terrorist network. They then employ a "key nodes" methodology to identify these high value targets within them that serve critical functions. OFAC believes that by eliminating these key nodes or high value targets the network would be disabled because without them the network would not receive sustaining services such as recruitment; training; logistical, material, financial, or technological support; and leadership. OFAC selects specific targets to recommend for designation based on the potential to cripple or otherwise dramatically impair the operations of the overall network by economically isolating these nodes. Economic sanctions are most effective against key nodes such as donors; financiers (fundraisers, financial institutions, and other commercial enterprises); leaders; charities; and facilitators such as logisticians. OFAC already has targeted key nodes in terrorist networks in several areas of the world including groups in Southeast Asia and various parts of Africa. OFAC is currently engaged in new research on groups in the Middle East, including Iraq, and the Caucasus.

A completed OFAC evidentiary record on a particular target is submitted first for legal review, then to the Executive Office of Terrorist Finance and Financial Crimes, where OFAC officers work with that office to prepare the package for the Policy Coordinating Committee (PCC). The PCC determines whether the USG should designate a particular entity or should pursue alternative legal or diplomatic strategies in order to achieve U.S. interests. As part of the PCC process, OFAC's designation proposal will usually be vetted by the consultative parties specified by the EO.

In addition to the evidentiary package, OFAC and other Treasury officers work with the interagency community to draft an unclassified Statement of the Case (SOC) which serves as the factual basis for the public announcement of a designation. The State Department uses it to pre-consult with countries which are directly impacted by a proposed US action and to urge them to designate at the same time as the USG. Upon a USG determination to designate, the SOC is used to notify host countries and the UN of an impending US action. It is also used to propose the inclusion of the target on the consolidated list of the UN 1267 Sanctions Committee of those individuals or entities associated with al Qaida or the Taliban.

UN and Bilaterally Proposed Designations

Whenever an individual or entity is proposed for inclusion on the UN 1267 consolidated list by another country through the UN or is proposed to the USG bilaterally, OFAC, and when appropriate the Department of State, is responsible for preparing the administrative record. In order to designate a target proposed to the UN by a Member State or by another government bilaterally to the USG, OFAC (or when appropriate State) must develop an administrative record that would support a domestic designation under E.O. 13224 as described above. Quite often, due to a difference in legal authorities and the type of or lack of information provided by a proposing country, this process may require several discussions with the initiating party and often requires further coordination through the UN and with other countries in order to obtain sufficient information to meet domestic legal criteria.

Other Counter-terrorism Activities

OFAC's role in the counter-terrorism arena is not limited to preparing designations, although this often serves as a key component of its other activities. The transnational nature of terrorism support networks requires engagement with allies and routine information sharing. OFAC's direct engagement with allies on terrorism support infrastructure began with officials from Saudi Arabia, Kuwait and the UAE in June 1999. Information and understandings developed from this and other OFAC trips to the region significantly contributed to formulating some of the strategies employed today.

Direct Treasury and OFAC engagement with foreign allies' counterparts provides an opportunity for OFAC to gather information, apply pressure, request support, or offer assistance. In some cases, Treasury may seek joint action with an ally in an effort to disrupt or dismantle an organization. In other instances, OFAC may use the threat of designation to gain cooperation, forcing key nodes of financial support to choose between public exposure of their support for terrorist activity or their good reputation.

Of course, OFAC also collaborates extensively with other elements within the Treasury Department. In particular, I want to mention our excellent relationship with IRS Criminal Investigation. This relationship has been especially important and productive in carrying out the Treasury Department's authority under Executive Order 13315, which blocks the assets of Saddam Hussein and other senior officials of the former Iraqi regime. For many months now, OFAC has been coordinating almost daily with Washington-based IRS-CI agents to guide the efforts of IRS-CI agents on the ground in Iraq to identify the ill-gotten assets of Saddam and his cronies. OFAC's partnership with IRS-CI on this issue has developed important investigational leads that would have been impossible if our organizations had not been so closely synchronized.

Significant OFAC Designations Pursuant to EO 13224

The result of OFAC's research and coordination efforts over the past three years has been several significant designations of charities, terrorist financiers, and financial support networks.

OFAC Actions against Terrorist-Supporting Charities:

- Holy Land Foundation (HLF). OFAC/IPD worked closely with the FBI prior to 9/11 to designate this charity located in Richardson, Texas. HLF was a financial supporter of HAMAS, a terrorist group originally designated in January 1995 pursuant to Executive Order 12947. The FBI Dallas field office specifically sought OFAC's involvement in its investigation and an OFAC/IPD officer became part of the North Dallas Terrorism Task Force. As a result of this close coordination, on December 4, 2001, OFAC designated the Holy Land Foundation pursuant to EO 13224 and EO 12947. This designation was upheld in U.S. Federal district court, affirmed on appeal, and on March 1, 2004, the Supreme Court denied HLF's petition for certiorari in HLF's challenge to its designation. Additionally, Section 501(p) of the Internal Revenue Code was enacted as part of the Military Family Tax Relief Act of 2003 (P.L. 108-121), effective November 11, 2003. Section 501 (p)(1) suspends the exemption from tax under section 501(a) of certain organizations, including those designated as a terrorist organization or foreign terrorist organization. Section 501(p), as a result, suspended HLF's tax exempt status (effective on the date of enactment of this section or the designation, which ever is later in time). This suspension continues until all designations and identifications of the organization are rescinded under the law or Executive Order under which such designation or identification was made.

- Benevolence International Foundation (BIF) & Global Relief Foundation (GRF) Blocking in Aid of Investigation. On December 14, 2001, the Treasury blocked pending investigation (BPI) the property of both BIF and GRF, two Islamic charities in Chicago, Illinois and the first such action under EO 13224. After the December 2001 BPI action, OFAC continued to work with other components of the Treasury and the FBI, SFOR in the Balkans, the Department of Justice, and the intelligence community to obtain additional information which led to the designation of GRF on October 17, 2002 and BIF on November 18, 2002 pursuant to EO 13224. On February 25, 2003 the civil lawsuit filed by BIF against the U.S. was voluntarily dismissed with prejudice and without costs. On November 12, 2003, the Supreme Court denied certiorari in GRF's appeal of the denial of its motion for preliminary injunction. As a result of the OFAC designation, IRS suspended the tax-exempt status of both BIF and GRF.

- Al Haramain Foundation. Treasury has worked closely with other U.S. Government agencies and Government of Saudi Arabia in order to coordinate the bilateral designation of six branches of this prominent Saudi charitable organization. The Bosnian and Somali branches were designated on March 11, 2002, the Pakistani, Indonesian, Kenyan, and Tanzanian branches were designated on January 22, 2004 and, most recently, the Albanian, Afghani, Bangladeshi, Ethiopian and Netherlands branches, as well as Al Haramain's former leader Aqeel Abdulazia Al-Aqil, were designated on June 2, 2004.

OFAC Actions against Terrorist Financial Networks:

- Al-Barakaat network. OFAC identified the Al-Barakaat Network as a major financial network providing material, financial, and logistical support to Usama Bin Laden, al Qaida, and other terrorist groups. On November 7, 2001, the President announced the designation of the Al-Barakaat Network pursuant to EO 13224. This action was taken in coordination with the predecessor to the Department of Homeland Security's ICE, the then Treasury Department's US Custom's Office of Investigation, which executed simultaneous search warrants at the time of designation. As a result of that action, Barakaat's cash flow was severely disrupted and the Emiratis closed down Barakaat's offices in their territory, froze its accounts, and placed several individuals under an informal house arrest. Since the designation, six Barakat-related individuals and entities were removed from the list upon demonstrating and ensursing that they were no longer engaging in the activities for which they were originally designated.

- Nada-Nasreddin / al Taqwa network. OFAC coordinated with U.S. law enforcement and intelligence community, and worked closely with its foreign partners in the Caribbean and Europe to target al Qaida supporters, Yousef Nada and Ahmed Idris Nasreddin. OFAC designated them and related companies in November 2001 and August 2002 pursuant to EO 13224, significantly disrupting another network.

- Wa'el Hamza Julaidan. OFAC identified Julaidan as a senior figure in the Saudi charitable community, who provided financial and other support, to several terrorist groups affiliated with al Qaida operating primarily in the Balkans. OFAC worked with other U.S. Government agencies and the Government of Saudi Arabia to coordinate a bilateral designation of Julaidan on September 6, 2002.

OFAC's Key Node Strategy

Over the past year and a half, OFAC has sought to take a more systematic approach to evaluating the activities of major terrorist organizations in various regions. This approach has focused on identifying "key nodes" discussed above, which when targeted and economically isolated can cripple a terrorist network's ability to function.

To implement this approach, OFAC staff has established collaborative relationships with several Department of Defense agencies and combatant commands in order to gain wider access to information critical to developing evidentiary records in support of designations. Working with DOD Commands and other DOD agencies provides OFAC and its DOD partners a force multiplier that brings together a variety of counterterrorism tools and resources. This will be an important model of inter-agency coordination as well as strategic vision for the Treasury Department as a whole, as we move toward greater integration and amplification of our intelligence and analysis functions in the Office of Intelligence and Analysis.

- Jemmah Islamiyah (JI) / Southeast Asia. In October 2002, OFAC began a joint project with the U.S. Pacific Command (USPACOM) and other DOD elements that identified terrorist support networks in Southeast Asia and selected key nodes, or priority targets, in these networks. The project's geographic scope included Indonesia, the Philippines, Malaysia and Singapore, and eight terrorist or Islamic extremist groups. The project focused special attention on the al Qaida-affiliated JI, the Abu Sayyaf Group (ASG), and the Moro Islamic Liberation Front (MILF), because of their relative importance in the region and threat to U.S. interests. The project identified the key leaders, fundraisers, businessmen, recruiters, companies, charities, mosques, and schools that were part of the JI support network. OFAC has sought to expand on this model through collaboration with other DOD agencies including the combatant commands. These efforts have included:

- The Horn of Africa. OFAC analysts have worked with DOD agencies, including analysts from the Office of Naval Intelligence (ONI), to fully identify the terrorism support infrastructure in the Horn of Africa. In this region, shipping and related drug smuggling activities appear to be strengthening the terrorism infrastructure. In coordination with our interagency partners, we were able to identify some of the key leaders, charities, and businesses that appear to be critical to the overall functioning of the network. In January 2003, the U.S. took joint action with the Government of Saudi Arabia against two of these key targets--the Kenya and Tanzania offices of the Saudi-based Al-Haramain Islamic Foundation.

- North Africa. In August 2003, I visited the U.S. European Command headquarters (USEUCOM) and met with the Chief of Staff, to begin a joint project including USEUCOM, OFAC officers, and other DOD elements to identify terrorist support networks in the North Africa region and key nodes within this network. The geographic scope of this project includes Morocco, Algeria, Tunisia, Libya, Mauritania, and Mali, and nine terrorist or Islamic extremist groups and their support networks. At the inception of this project, the Director of USEUCOM's Intelligence Directorate indicated that this region posed the most serious threat in USEUCOM's area of responsibility and asked OFAC to devote available resources to the project. The recent Madrid bombings and the suspicion that North African terrorists may have been involved illustrates the reality of the threat these groups pose not only to the stability of the region but the interests of the U.S. and our allies.

- Caucasus. In January 2004, the USEUCOM Chief of Staff visited OFAC and was briefed on an OFAC initiative to identify terrorist groups and their support networks in another region of USEUCOM's area of responsibility. The Chief of Staff invited an OFAC analyst to USEUCOM's Joint Analysis Center in Molesworth, England, to work with a regional analyst there to further develop information on terrorist activity in the region. The outcome of the week-long visit was that it confirmed our preliminary analytical conclusions of terrorist activity and support. We are now in discussion with a DOD element, USEUCOM, and a U.S. Government agency to pursue a collaborative effort to refine our understanding and determine if the initiative justifies the commitment of limited resources for the ultimate exercise of OFAC sanctions or other appropriate U.S. Government authorities against priority targets we may identify.

- Additional Initiatives. In March of this year, OFAC was invited to brief the Headquarters North American Aerospace Defense Command (NORAD) and U.S. North Command (USNORTHCOM) Interagency Coordination Group (JIACG) on the subject of OFAC authorities under Executive Order 13224 and OFAC efforts against terrorism. In addition, the U.S. Southern Command (USSOUTHCOM) has also contacted my office and expressed an interest in an OFAC analyst detailed to the USSOUTHCOM JIACG. OFAC continues to explore collaborative opportunities with both of these commands.

These efforts have been so successful that, in December 2003, the Office of the Secretary of Defense requested the detail of six OFAC employees to the headquarters of six DOD combatant commands. As a result, we hope to detail OFAC analysts with the U.S. Central Command (USCENTCOM) and U.S. Special Operations Command (SOCOM) in the near future.

OFAC Attaché Offices and Foreign Counterparts

OFAC's ability to successfully pursue counter-narcotics and counter-terrorism missions has been greatly enhanced by assigning OFAC officers to attaché and liaison positions abroad with several US embassies and military commands

- **OFAC Bogotá office** coordinates OFAC sanctions programs in Colombia and conducts research on Colombian drug cartels and narco-terrorists. The OFAC Attaché and Assistant Attaché in Bogota serve as the liaison with U.S. Embassy elements and Colombian government agencies and have established solid relationships with the Colombian banking and private sectors. OFAC/IPD officers travel regularly to Colombia and have extensive knowledge of Colombian drug cartel finances.

- **OFAC Mexico City office** coordinates OFAC sanctions programs in

- Compliance is building a new Specially Designated Nationals database that will allow enterprise-wide access to declassified target information and permit analysts to directly link from a name on the SDN list to the underlying declassified evidentiary material for easy access.

- Compliance intends, in the near future, to make a new DataMart feature available on the OFAC website that will allow users of OFAC's Specially Designated Nationals list to more easily "shop" for information that is tailored to their specific compliance needs.

Licensing Division

- OFAC's Licensing Division plans to further increase the efficiency with which license applications and requests for interpretive rulings are processed, with a goal of no longer than a two-week turnaround for submissions, which do not require review and clearance outside the Division.

- Licensing intends to develop enhanced capabilities for scanning and e-mail connectivity to facilitate review and clearance of licensing submissions requiring interagency consultation, with the ultimate goal of developing a web-based system with interagency access to avoid the need to transmit material altogether.

- The Division also plans to develop and publish on OFAC's website "treatises" on the various categories of commercial and financial transactions subject to OFAC's jurisdiction. These treatises will discuss OFAC's licensing practices with regard to the application of OFAC's regulations to those transactions. Redacted versions of the Division's interpretive rulings will be appended to the relevant treatise, providing comprehensive guidance and promoting consistency and transparency with respect to subjects ranging from trade issues and financial instruments and services to ownership and control and acquisition and divestiture.

- Licensing will continue supporting OFAC's regulatory implementation function by participating in the preparation of draft regulations and promoting their timely clearance and publication.

Enforcement Division

- Enforcement will build on and improve upon OFAC's existing relationships with federal law enforcement agencies, principally the FBI, ICE, Customs and Border Protection, Commerce Office of Export Enforcement and Offices of the United States Attorney, to enhance the criminal enforcement of OFAC sanctions programs.

International Programs (Counter-Narcotics) Division

- · OFAC's continuing counter-narcotics designation program objectives are to identify, expose, isolate, and incapacitate the business and financial infrastructures and penetrations into the legitimate economy of foreign narcotics kingpins and drug cartels, as well as their agents and functionaries. OFAC will continue to develop its working relationships with federal law enforcement agencies, U.S. Attorneys' offices, intelligence community elements, military commands, and select foreign enforcement and counter-narcotics units on a global basis.

OFAC will continue to develop operational relationships in the field and at headquarters with Federal law enforcement agencies, U.S. Attorneys' offices, Intelligence Community elements, and military commands. This includes more personnel to work with OCDETFs and other operational task forces and more training of the other government components in OFAC narcotics designation programs.

OFAC also plans to increase its participation in narcotics fusion and targeting centers and related interagency programs.

Foreign Terrorism Programs Division

OFAC plans to continue to expand its efforts to impede the activities of terrorist organizations utilizing the key nodes methodology. This will be done in concert with the new Office of Intelligence Analysis (OIA), as the Treasury Department works to integrate its analytical work product with all components of Treasury and the intelligence community. The new OIA will work with OFAC to monitor all relevant intelligence which can be used to further OFAC's mission. OFAC, using this information as well as other sources and its own research, will continue to develop the structure of terrorist groups and their support networks and to identify and isolate key nodes within them that serve critical functions, building upon and continuing the work with the military commands.

- OFAC will seek to detail OFAC officers to six DOD combatant commands for periods of two years to exploit the unique DOD resources and abilities to identify terrorists, terrorist groups, and their support networks, including DOD analytic resources, data collection, and most importantly local knowledge.

IT Challenges

Improving OFAC's Information Technology capabilities remains one of the greatest challenges to enhancing OFAC's ability to pursue its mission. OFAC could enhance current analytical capabilities by utilizing more advanced and available information technologies and advanced communications capabilities. Communication and cooperation with participating unified military combatant commanders and civil agencies has shown great promise in sharing information resources to identify terrorist targets, non-state enemies that function within worldwide terrorist networks demands closer coordination by U.S. government agencies and military in the diplomatic, economic, intelligence, and law enforcement domains. To enhance its capabilities, OFAC is pursuing the following communication systems and technologies that would enable the coordination and integration that is critical for agencies, military forces, and coalition nations to effectively fight in this new war:

- **Database Application**. OFAC could improve its ability to share and store information with the development of an internal database application. This application would reside on the "classified" networks and allow OFAC analysts to store and analyze information. This information could be shared, as appropriate, through classified communication networks and provide participating partners (Intelligence Community, Military Commands, and

Law Enforcement Agencies) with substantive targeting information.

- **Enhanced electronic communication.** This includes the establishment of a multi-media infrastructure using the Defense Messaging System cable communications servers, web servers, secure email, and data servers using Public Key Infrastructure (PKI) and FORTEZZA national security information assurance for both the Joint Worldwide Intelligence Communication System (JWICS) and the Secret IP Router Network (SIPRNET) enclaves. Establishing connectivity to the DOD interoperability of secure voice and data during periods of heightened protection requiring rapid analytical reporting between military and civil agencies.

- **Establishment of a robust e-mail system and database infrastructure.** OFAC will establish a robust e-mail system and database infrastructure for the exchange of Sensitive But Unclassified (SBU) information with the U.S. and international partner law enforcement community. This infrastructure would take advantage of emerging technologies with respect to repudiation with digital signature, authentication, and PKI information assurance protections. The access of law enforcement databases (NLETS, TECS, etc) for the cross-analytical work required between intelligence and law enforcement sensitive data. This enhanced communications capability will allow OFAC to exploit "open to government" information sources.

- **Developing Secure Video Teleconferencing (SVTC) capabilities**. OFAC is in the process of developing and enhancing its SVTC capbilities on both the JWICS for intelligence and SIPRNet for sanitized information of a law enforcement nature. Completion of construction on OFAC's Secure Video Teleconferencing facility will allow officers in Washington to communicate and work more effectively on joint projects involving civil agencies and U.S. military and coalition forces. Ensuring the collaborative strategic planning of a host of entities in the conduct of counter-terrorism and counter-narcotic missions.

- **Better Communication Utilizing SIPRNET and ADNET Enclaves.** Both the International Programs Division (counter-narcotics) and the Foreign Terrorist Programs Division (counter-terrorism) will seek to improve their electronic communication with the law enforcement community by utilizing systems as SIPRNET and the Anti Drug Network (ADNET).

Increased OFAC Cooperation with Foreign Counterparts

- OFAC's trips to target areas and its discussions with its counterparts in other countries have afforded OFAC the opportunity to work with these partners and provide guidance on the sanction strategies it currently employs. In all these, and future efforts, Treasury, working in coordination with other U.S. government agencies including the State Department, will take advantage of OFAC contacts and work abroad to increase cooperative efforts and expand its interaction with other government counterparts in order to deal with common threats against the United States and our allies.

Madame Chairman, I would like to thank you and the Committee for the opportunity to speak on these issues. This concludes my remarks today. I will be happy to answer your questions.

Exhibit 9

PRESS ROOM
U.S. DEPARTMENT OF THE TREASURY

FROM THE OFFICE OF PUBLIC AFFAIRS

February 19, 2004
JS-1183

Treasury Announces Actions Against AL-Haramain

The United States Attorney's Office for the District of Oregon announced a federal search warrant was executed yesterday against property purchased on behalf of the Al Haramain Islamic Foundation, Inc. in Ashland, Oregon.

The search was led by agents of the Internal Revenue Service-CI as part of a joint Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS)/Immigration and Customs Enforcement investigation.

This search was conducted pursuant to a criminal investigation into possible violations of the Internal Revenue Code, the Money Laundering Control Act and the Bank Secrecy Act. The suspected crimes relate to possible violations of the currency reporting and tax return laws by two officers of the Ashland Oregon office of Al Haramain Foundation, Inc.

In a separate administrative action today, the Treasury's Office of Foreign Assets Control (OFAC) has blocked pending investigation accounts of the Al Haramain Foundation, Inc. to ensure the preservation of its assets pending further OFAC investigation.

The parent of the Oregon Al Haramain Islamic Foundation is headquartered in Saudi Arabia, and is one of that country's largest Non Governmental Organizations, with worldwide reach.

In March 2002, the United States Treasury and the Kingdom of Saudi Arabia jointly designated the Bosnian and Somalia Branches of Al Haramain as supporters of terrorism. In December 2003, the reconstituted branch of Al Haramain in Bosnia, Vazir, was also designated by both governments as a supporter of terrorism. In January 2004, the Kingdom of Saudi Arabia and the U.S. Department of the Treasury jointly designated four additional Al Haramain branches – Indonesia, Tanzania, Kenya and Pakistan – as being supporters of terrorism. The United Nations has adopted these Al Haramain designations and imposed an asset freeze, travel ban and arms embargo pursuant to United Nations Security Council Resolutions 1267/1390/1455.

Exhibit 10

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

APR 23 2004

Lynne Bernabei
Bernabei & Katz, PLLC
1773 T Street, NW
Washington, D.C. 20009-7139

Re: Al Haramain Islamic Foundation, Inc.

Dear Ms. Bernabei:

Based on the enclosed unclassified information and on classified documents that are not authorized for public disclosure, including disclosure to you or your client, the al Haramain Foundation, the Office of Foreign Assets Control ("OFAC") is considering designating the Al Haramain Foundation branch office in Oregon ("AHF") as a Specially Designated Global Terrorist pursuant to Executive Order 13224 and the International Emergency Economic Powers Act, 50 U.S.C. § 1701 *et seq*. Material covered by privilege as well as private information about government employees was redacted. If OFAC considers any additional unclassified material, it will forward that information to you for your review. Any material that AHF may wish to submit to OFAC in response to this letter must be received within 21 days of the date of this letter, to allow the agency an opportunity to evaluate that information prior to making the designation determination.

The response to this notice should be directed to R. Richard Newcomb, Director, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Annex, Washington, D.C. 20220. A copy of your response also should be provided to Ms. Cari Stinebower in Chief Counsel's Office (Foreign Assets Control). If you have any questions, please contact Cari Stinebower at (202) 622-2410.

Sincerely,

Richard Newcomb

R. Richard Newcomb
Director
Office of Foreign Assets Control

Enclosures

cc: Andrea Gacki

Exhibit 11

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

FAC No. SDG 229662

JUL 2 3 2004

Lynne Bernabei
Bernabei & Katz, PLLC
1773 T Street, NW
Washington, D.C. 20009-7139

Re: Al Haramain Islamic Foundation, Inc.

Dear Ms. Bernabei:

As a follow-up to my April 23, 2004 letter to you, I am informing you that the Office of Foreign Assets Control (OFAC) is considering (1) the attached additional unclassified material, (2) the material provided to you on April 23 or referenced in the April 23 letter, (3) additional classified information not being provided to you, (4) correspondence between OFAC and al Haramain Islamic Foundation, Inc. ("AHF"), and (5) material you have provided for inclusion in the record, in determining whether to designate AHF, as a Specially Designated Global Terrorist pursuant to Executive Order 13224 and the International Emergency Economic Powers Act, 50 U.S.C. §§ 1701-06. All of the information described in the April 23 letter and in this letter, any material that AHF submits to OFAC in response, and all correspondence between OFAC and AHF will constitute the administrative record upon which OFAC will make its designation determination. Any material that AHF may wish to submit to OFAC in response to this letter must be received within 7 days of the date of this letter, to allow the agency an opportunity to evaluate that information prior to making the designation determination.

The response to this notice should be directed to R. Richard Newcomb, Director, Office of Foreign Assets Control, U.S. Department of the Treasury, 1500 Pennsylvania Avenue, N.W., Annex, Washington, D.C. 20220. A copy of your response also should be provided to Ms. Cari Stinebower in Chief Counsel's Office (Foreign Assets Control). If you have any questions, please contact Cari Stinebower at (202) 622-2410.

Sincerely,

Richard Newcomb

R. Richard Newcomb
Director
Office of Foreign Assets Control

Enclosures

Exhibit 12

PRESS ROOM
U.S. DEPARTMENT OF THE TREASURY

FROM THE OFFICE OF PUBLIC AFFAIRS

September 9, 2004
JS-1895

U.S.-Based Branch of Al Haramain Foundation Linked to Terror
Treasury Designates U.S. Branch, Director

The Treasury Department announced today the designation of the U.S. branch of the Saudi Arabia-based Al Haramain Islamic Foundation (AHF), along with one of its directors, Suliman Al-Buthe. In addition, the AHF branch located in the Union of the Comoros was also designated today.

"We continue to use all relevant powers of the U.S. government to pursue and identify the channels of terrorist financing, such as corrupted charities, at home and abroad. Al Haramain has been used around the world to underwrite terror, therefore we have taken this action to excommunicate these two branches and Suliman Al-Buthe from the worldwide financial community," said Stuart Levey, Treasury's Under Secretary for Terrorism and Financial Intelligence.

The assets of the U.S. AHF branch, which is headquartered in Oregon, were blocked pending investigation on February 19, 2004. On the previous day, a federal search warrant was executed against all property purchased on behalf of the U.S. AHF branch. The investigation involved agents from the Internal Revenue Service – Criminal Investigations (IRS-CI), the Federal Bureau of Investigation (FBI) and the Department of Homeland Security's Immigration and Customs Enforcement (ICE).

The U.S.-based branch of AHF was formally established in 1997. Documents naming Al-Buthe as the organization's attorney and providing him with broad legal authority were signed by Aqeel Abdul Aziz Al-Aqil, the former director of AFH. Aqil has been designated by the United States and the UN 1267 Sanctions Committee because of AHF's support for al Qaida while under his oversight.

The investigation shows direct links between the U.S. branch and Usama bin Laden. In addition, the affidavit alleges the U.S. branch of AHF criminally violated tax laws and engaged in other money laundering offenses. Information shows that individuals associated with the branch tried to conceal the movement of funds intended for Chechnya by omitting them from tax returns and mischaracterizing their use, which they claimed was for the purchase of a prayer house in Springfield, Missouri.

Other information available to the U.S. shows that funds that were donated to AHF with the intention of supporting Chechen refugees were diverted to support mujahideen, as well as Chechen leaders affiliated with the al Qaida network.

AHF has operations throughout the Union of the Comoros, and information shows that two associates of AHF Comoros are linked to al Qaida. According to the transcript from U.S. v. Bin Laden, the Union of the Comoros was used as a staging area and exfiltration route for the perpetrators of the 1998 bombings of the U.S. embassies in Kenya and Tanzania. The AHF branches in Kenya and Tanzania have been previously designated for providing financial and other operational support to these terrorist attacks.

Since March 2002, the United States and Saudi Arabia have jointly designated eleven branches of AHF based on evidence of financial, material and/or logistical support to the al Qaida network and affiliated organizations. These branches, Afghanistan, Albania, Bangladesh, Bosnia, Ethiopia, Indonesia, Kenya, the

Netherlands, Pakistan, Somalia, and Tanzania, along with the former director of AHF, Aqeel Abdul Aziz Al-Aqil, are named on the UN's 1267 Committee's consolidated list of terrorists associated with al Qaida, Usama bin Laden and the Taliban and are subject to international sanctions.

The entities were designated today pursuant to Executive Order 13224 pursuant to paragraphs (d)(i) and (d)(ii) based on a determination that they assist in, sponsor or provide financial, material, or technological support for, or financial or other services to or in support of, or are otherwise associated with, persons listed as subject to E.O. 13224. These entities also meet the standard for inclusion in the UN 1267 Sanctions Committee's consolidated list because of the support provided to UBL, al Qaida or the Taliban.

Inclusion on the 1267 Committee's list triggers international obligations on all member countries, requiring them to freeze the assets of these offices. Publicly identifying these supporters of terrorism is a critical part of the international campaign to counter terrorism. Additionally, other organizations and individuals are put on notice that they are prohibited from doing business with them.

Blocking actions are critical to combating the financing of terrorism. When an action is put into place, any assets existing in the formal financial system at the time of the order are to be frozen. Blocking actions serve additional functions as well, acting as a deterrent for non-designated parties who might otherwise be willing to finance terrorist activity; exposing terrorist financing "money trails" that may generate leads to previously unknown terrorist cells and financiers, disrupting terrorist financing networks by encouraging designated terrorist supporters to disassociate themselves from terrorist activity and renounce their affiliation with terrorist groups; terminating terrorist cash flows by shutting down the pipelines used to move terrorist-related assets; forcing terrorists to use alternative, more costly and higher-risk means of financing their activities; and engendering international cooperation and compliance with obligations under UN Security Council Resolutions.

The United States has designated 387 individuals and entities as terrorists, their financiers or facilitators. In addition, the global community has frozen over $142 million in terrorist-related assets.

Al Haramain Islamic Foundation – United States

1257 Siskiyou Blvd.
Ashland, Oregon 97520

3800 Highway 99 S
Ashland, Oregon 97520

2151 E. Division Street
Springfield, MO 65803

Al Haramain Islamic Foundation – Union of the Comoros

B/P: 1652 Moroni
Union of the Comoros

Suliman Al-Buthe
DOB: 12/08/1961
POB: Egypt
Nationality: Saudi Arabian
Passport No: B049614

For more information on the February 19, 2004 designation of the U.S.-based AHF branch, please visit: http://www.treasury.gov/press/releases/js1183.htm.

Note: In June of 2004, the Saudi government announced it was dissolving AHF and other Saudi charities and committees operating aboard and folding their assets into a newly created entity, the Saudi National Commission for Relief and Charity Work Abroad. According to the Saudi Embassy, the Commission, which will be a non-governmental body, will take over all aspects of private overseas aid operations and assume responsibility for the distribution of private charitable donations from Saudi Arabia.